

BACHELORARBEIT

zur Erlangung eines akademischen Grades eines

Bachelor of Engineering (B.Eng.)

im Studiengang **Geoinformationen** im Studienschwerpunkt **Geodäsie**

Jamming von GNSS –

**Ein Überblick über Methoden, Auswirkungen und
Gegenmaßnahmen in verschiedenen Anwendungsbereichen**

vorgelegt von

Hanna Nonhoff (Matrikel-Nr.: 955713)

im Sommersemester 2025 in Berlin

Betreuerin: Prof. Dr.-Ing. Jessica Glabsch

2. Gutachter: Prof. Dr.-Ing. Boris Resnik

I Eidesstattliche Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe angefertigt und mich anderer als der in den beigefügten Verzeichnissen angegebenen Hilfsmittel nicht bedient habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen wurden, sind als solche kenntlich gemacht. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht. Ich bin mir bewusst, dass eine unwahre Erklärung rechtliche Folgen hat.

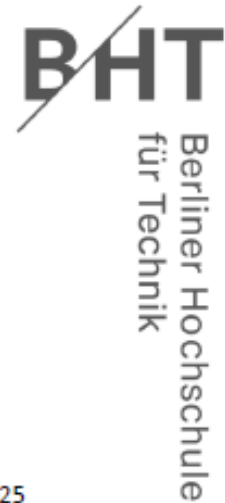
Berlin, 22.07.2025

H. Nonhoff

Ort, Datum, Unterschrift

II Aufgabenstellung

Berliner Hochschule für Technik, Luxemburger Straße 10, 13353 Berlin



29. April 2025

Bachelorarbeit im Sommersemester 2025

Hanna Nonhoff (Matrikelnummer 955713)

„Jamming von GNSS - Ein Überblick über Methoden, Auswirkungen und Gegenmaßnahmen in verschiedenen Anwendungsbereichen“

GNSS (Global Navigation Satellite System) ist ein vielseitig einsetzbares System um die Koordinaten von Punkten zu bestimmen. Es wird in der Positionierung und Navigation nicht nur von Fahrzeugen verwendet. Jamming und Spoofing spielt eine immer bedeutendere Rolle unter anderem im Bereich Navigation Warfare aufgrund der damit einhergehenden Manipulation des GNSS.

Die wesentliche Aufgabe der Bachelorarbeit ist die Methoden sowie die Auswirkungen von Jamming und Spoofing auf die Positionen zu erläutern und möglichen Gegenmaßnahmen darzustellen.

In der Bachelorarbeit müssen folgende Teilbereiche bearbeitet werden:

1. Literaturrecherche zu den theoretischen Grundlagen von GNSS
2. Literaturrecherche zu Störungsquellen beim GNSS
3. Anwendungsbeispiele von Jamming und Spoofing
4. Detektion von Jamming und Spoofing und mögliche Gegenmaßnahmen
5. Mögliche Alternativen zum GNSS
6. Bewertung der Auswirkungen sowie der möglichen Alternativen
7. Fazit

Beginn der Arbeit: SoSe 2025

Bei der Bearbeitung der Aufgabenstellung ist darauf zu achten, dass die Vorgehensweise eingehend erläutert, alle getroffenen Entscheidungen gut begründet und die Ergebnisse übersichtlich zusammengestellt werden. Dazu gehört auch, dass aufgetretene technische Probleme sachlich dokumentiert werden. Wichtig ist darüber hinaus, dass die erzielten Ergebnisse anhand nachvollziehbarer Kriterien evaluiert und kritisch bewertet werden.

Prof. Dr.-Ing. Jessica Glöbsch
Fachbereich III – Bauingenieur- und
Geoinformationswesen
Haus Bauwesen Raum D 444
jessica.gloeb@bht-berlin.de

Berliner Hochschule für Technik
Luxemburger Straße 10
13353 Berlin



Studiere Zukunft

Die Abschlussarbeit ist in regelmäßiger Abstimmung mit dem Betreuer zu erstellen. Spätestens 1 Woche nach Ausgabe der Aufgabenstellung ist die Arbeit und die Bearbeitung mit dem Betreuer bei einem Termin persönlich abzustimmen. Weitere Abstimmungstermine sind anschließend regelmäßig gem. Betreuungsplan gem. RSPO und nach Bedarf mit dem Betreuer durchzuführen.

Verzögerungen in der Datenbereitstellung durch Dritte und damit einhergehende zeitliche Verzögerungen oder Einschränkungen bzgl. der Bearbeitung im Sinne dieser Aufgabenstellung sind unverzüglich dem Betreuer und ggf. dem Prüfungsausschuss anzuzeigen.

Die Bachelorarbeit stellt eine wissenschaftliche Arbeit dar; die formalen und formellen Anforderungen an eine wissenschaftliche Arbeit sind zu beachten.

Die Abschlussarbeit und die erzielten Analyseergebnisse sind zusätzlich zu den Vorgaben der Prüfungsordnung in digitaler Form (Word-Dateien, Datenkopien, programmspezifische Berechnungsdateien, etc.) strukturiert, vollständig und nachvollziehbar abzugeben. Es wird empfohlen, der Prüfungskommission zwei gedruckte und gebundene Exemplare der Abschlussarbeit zur Verfügung zu stellen.

Der Bearbeitungszeitraum beträgt gem. RSPO 3 Monate.

Zur öffentlichen Präsentation der Arbeit ist ein Poster mit den wichtigsten Ergebnissen anzufertigen.



Jessica Glabsch

III Vorbemerkung

Diese Bachelorarbeit wird zum Abschluss meines Studiums an der Berliner Hochschule für Technik im Studiengang Geoinformationen mit dem Schwerpunkt Geodäsie verfasst.

An dieser Stelle möchte ich mich bei allen bedanken, die mich im Rahmen meiner Bachelorarbeit sowohl fachlich als auch persönlich unterstützt haben. Ein besonderer Dank geht an Frau Prof. Dr.-Ing. Jessica Glabsch für die fachliche Unterstützung und Betreuung der Bachelorarbeit. Sowie an das Dezernat V (1) des Zentrums für Geoinformationswesen der Bundeswehr für die fachliche Unterstützung, besonders auch an den Dezernatsleiter Herrn Oberstleutnant Markus Vogt sowie Herrn Major René Anger für die Ermöglichung und Betreuung des Praktikums im Rahmen der Bachelorarbeit.

Des Weiteren danke ich meinen Freunden und Kommilitonen Melissa Bork, Vivien Kano, Kristina Rassau, Konstantin Wiedemann und Jonas Woddow für die gemeinsame Zeit des Studiums und all die gegenseitige Motivation. Ein großer Dank gilt meinen Freunden und meiner Familie in der Heimat, die mir während des Studiums und der Bachelorarbeit den Rücken freigehalten haben.

Aus Gründen der Lesbarkeit wird in dieser Arbeit nach Rücksprache mit der Betreuerin auf eine geschlechtsneutrale Formulierung verzichtet. Personenbezeichnungen gelten, wenn nicht anders gekennzeichnet, im Sinne des generischen Maskulinums und schließen alle Geschlechter gleichermaßen ein. Diese Entscheidung dient der sprachlichen Klarheit und orientiert sich an wissenschaftlichen Schreibkonventionen, ohne Diskriminierung oder Wertung zum Ausdruck zu bringen. Die Gleichbehandlung aller Geschlechter wird unabhängig von der gewählten Schreibform als selbstverständlich erachtet.

IV Inhaltsverzeichnis

I Eidesstattliche Erklärung	i
II Aufgabenstellung	ii
III Vorbemerkung	iv
IV Inhaltsverzeichnis	v
V Abbildungsverzeichnis	vii
VI Formelverzeichnis	viii
VII Tabellenverzeichnis	viii
VII Abkürzungsverzeichnis	ix
1 Einleitung	1
2 GNSS	3
2.1 GNSS-Grundlagen	3
2.2 Anwendungsfelder von GNSS	10
2.2.1 Bodengestützte Anwendungen	11
2.2.2 Luftgestützte Anwendungen	12
2.2.3 Maritime Anwendungen	14
3 Störungen von GNSS-Signalen	15
3.1 Überblick der Arten	15
3.2 Beabsichtigte Störungen	18
3.2.1 Jamming	18
3.2.2 Spoofing	22
3.3 Ziviles und Militärisches Jamming und Spoofing	25
3.3.1 Ziviles Jamming und Spoofing	25
3.3.2 Jamming und Spoofing im militärischen Kontext	27
3.3.3 Navigation Warfare	29
3.3.4 Technische Umsetzung und Testszenarien	32
3.3.5 Geopolitische und sicherheitsrelevante Entwicklungen	37
4 Auswirkung von Jamming und Spoofing	39
4.1 Allgemein	39
4.2 Im zivilen und militärischen Kontext	40

4.3	In ausgewählten Bereichen.....	43
4.3.1	Auf bodengebundene Anwendungen.....	43
4.3.2	Auf luftgestützte Anwendungen	48
4.3.3	Auf maritime Anwendungen	52
5	Störungsmanagement	57
5.1	Detektion von Jamming und Spoofing	57
5.2	Schaffen von robustem GNSS	62
5.2.1	Funkbasierte Ortungssysteme und Systemintegration	62
5.2.2	Signalintegration und Antennentechnologie.....	63
5.2.3	Kryptographische Schutzmaßnahmen und Authentifizierung	65
5.2.4	Operative, strategische und gesellschaftliche Gegenmaßnahmen.....	67
5.3	Alternative Navigationsverfahren zum GNSS	68
5.3.1	Etablierte Verfahren und Systeme	68
5.3.2	Technologiekonzepte im Entwicklungsstadium.....	71
5.3.3	Resiliente Navigationsverfahren für Not- und Krisenszenarien	77
6	Zusammenfassung	79
7	Literaturverzeichnis	82

V Abbildungsverzeichnis

Abb. 2-1: GPS III SV01 Satellit (LOCKHEED 2019)	3
Abb. 2-2: Prinzip von Differentiellem GPS (erstellt nach SCHÜTTLER 2022)	5
Abb. 2-3: Elemente eines GNSS-Empfängers (BAUER 2017)	6
Abb. 2-4: mögliche Fehlereinflüsse auf GNSS (erstellt nach BAUER 2017, MANSFELD 2010)7	
Abb. 2-5: GNSS-Frequenzbereiche in unteren und oberen L-Band (BLUM 2022)	9
Abb. 2-6: mögliche Anwendungsbereiche (erstellt nach MANSFELD 2010).....	10
Abb. 2-7: Tsunami Warnsystem mittels GPS-Bojen (KATO et al. 2011).....	11
Abb. 2-8: Funktionsschema eines GPS-Landeanflugsystems (geändert nach MANSFELD 2010).....	13
Abb. 3-1: GNSS-Signale und Amateurfunk (erstellt nach BAUER 2017)	16
Abb. 3-2: Signalarten (geändert nach BLUM et al. 2023)	17
Abb. 3-3: Jammerklassifizierung (erstellt nach MEURER 2024).....	18
Abb. 3-4: Beeinflussung der Positionsbestimmung durch Jammer (erstellt nach MANSFELD 2010).....	19
Abb. 3-5: Abschaltung der SA am 02.05.2000 (geändert nach SOKOLOV 2020)	21
Abb. 3-6: Prinzip des Meanconing (geändert nach BLUM 2022)	23
Abb. 3-7: Personal Privacy Device der Bundeswehr (BLUM et al. 2023).....	26
Abb. 3-8: HP47+ (GUSENBURGER 2022)	28
Abb. 3-9: Zielsetzung NAVWAR (geändert nach MEURER 2024)	30
Abb. 3-10: Abschuss von Antisatellitenraketen (THEDARTHDESIGNER 2019).....	31
Abb. 3-11: Marschflugkörper Taurus (CARSTENSEN 2024).....	33
Abb. 3-12: Bewertungsablauf von GNSS-Störungen (geändert nach KO 2010).....	34
Abb. 3-13: Störung der GPS-L1-Frequenz auf 150m Entfernung zum Störsender (BLUM et al. 2023).....	36
Abb. 3-14: russisches Störsendersystem (SAPWOOD 2024).....	38
Abb. 4-1: Auswirkungen von Maut-Jamming (erstellt nach BAUER 2017).....	44
Abb. 4-2: Störauswirkungen auf Satellitenanzahl und Carrier to Noise Ratio (STANISAK et al. 2016).....	45
Abb. 4-3: Spoofing von autonomem Fahren (erstellt nach KUUSNIEMI 2022).....	46
Abb. 4-4: tägliche Anzahl der gespoofen Flüge pro vorgetäuschem Gebiet (SKAI DATA SERVICES 2025b).....	48
Abb. 4-5: Spoofing eines Flugzeuges (SKAI DATA SERVICES 2025a).....	49
Abb. 4-6: Zoom auf Ballungsraum Naher Osten (SKAI DATA SERVICES 2025a).....	49
Abb. 4-7: Jamming und Spoofing auf Flugzeuge am 09.06.2025 (SKAI DATA SERVICES 2025a).....	50

Abb. 4-8: Jamming und Spoofing auf Flugzeuge am 15.06.2025 (SKAI DATA SERVICES 2025a).....	50
Abb. 4-9: Abschuss von Loitering Munition (UNMANNED NETWORK 2023).....	51
Abb. 4-10: Kursabweichung durch Spoofing (KPLER 2025).....	53
Abb. 4-11: GPS-Interferenz im Ostseeraum (WISEMANN 2022).....	54
Abb. 4-12: Satellitenaufnahmen (BERGMANN et al. 2023).....	55
Abb. 4-13: AIS-Signale und Bewegungsdaten (BERGMANN et al. 2023).....	55
Abb. 5-1: Veränderung der Signalstärke durch AGC (BAUER 2017).....	57
Abb. 5-2: Veränderung der Korrelationsfunktion durch Jamming (BAUER 2017).....	59
Abb. 5-3: Verlauf der Doppler-Frequenzverschiebung mit und ohne Spoofing (BLUM 2022).....	60
Abb. 5-4: Künstliche Intelligenz basiertes Detektionschema von Jamming und Spoofing (GEWIES et al. 2024).....	61
Abb. 5-5: mögliche Anti-Jamming-Fähigkeiten (SCHMIDT 2013).....	65
Abb. 5-6: Pseudolite (geändert nach MEURER 2024).....	69
Abb. 5-7: Quenten-INS im Vergleich zu herkömmlichen INS (FUTUREZONE 2025).....	71
Abb. 5-8: BANSHEE (geändert nach VAL 2022).....	72
Abb. 5-9: Genauigkeit Mode-N (LANGLEY et al. 2021).....	74
Abb. 5-10: R-Mode Sender (LUFTFAHRTMAGAZIN 2025).....	75
Abb. 5-11: Positionsgenauigkeiten von UAV (BAO et al. 2025).....	76
Abb. 5-12: Sextant (RÖNNBERG 2020).....	77
Abb. 5-13: Karte und Kompass (LICKTEIG 2023).....	78

VI Formelverzeichnis

Formel 2-1: Pseudoentfernung (nach MANSFELD 2010).....	4
Formel 2-2: Strecke aus Trägerphasenmessung (BLUM 2022).....	4
Formel 2-3: Signal-zu-Rauschen-Quotient (BAUER 2017).....	8
Formel 2-4: Träger-zu-Rauschen-Dichte-Quotient (BAUER 2017).....	8
Formel 5-1: effektiver C/N_0 -Wert (BAUER 2017).....	58

VII Tabellenverzeichnis

Tabelle 3-1: Gegenüberstellung von Jamming und Spoofing.....	24
Tabelle 4-1: Bedrohungsmatrix von GNSS-Jamming (geändert nach RETERSKI 2015).....	42

VII Abkürzungsverzeichnis

ADC	Analog-digital-Wandler (engl. Analog-Digital-Converter)
AGC	Automatische Verstärkungsregelung (engl. Automatic Gain Control)
AIS	Automatic Identification System
ARGOS	Anti-theft Robust Galileo-based Operational System
ARNS	Aeronautical Radio Navigation Service
AS oder A/S	Anti-Spoofing
A/J	Anti-Jamming
C/A-Code	clear/acquisition Code
CISA	Certified Information Systems Auditor
CRPA	Controlled reception pattern antenna
CSAC	Chip-Scale Atomic Clock
C-Scan	Combines State-of-the-art Chip-scale Atomic Navigation
DARPS	Differential Absolute and Relative Positioning Sensor
DGPS	differentielles GPS
DLR	deutsches Zentrum für Luft- und Raumfahrt
DME	Distance Measuring Equipment
DOP	Dilution of Precision
EGNOS	European Geostationary Navigation Overlay Service
eLORAN	enhanced LORAN
ERP	effektiven Strahlungsleistung (engl. Equivalent Isotropic Radiated Power)
EW	elektronischen Kampfführung (engl. Electronic Warfare)
FFT	Fast-Fourier-Transformation
GBAS	bodengebundenes Ergänzungssystem (engl. Ground based Augmentation System)
GLONASS	GLOBALnaya NAVigatsionnaya Sputnikovaya Sistema
GNSS	globales Navigationssatellitensystem
GWPS	Ground Proximity Warning System
HALI	Finnisch: „HälytysAjoneuvojen LiikennevaloetuuDET“, auf Deutsch „Ampelsteuerung für Einsatzfahrzeuge“
IMU	inertialen Messdaten (engl. Inertial Measurement Unit)
INS	Inertiales Navigationssystem
J/S	Jamming-to-signal ratio
LDACS	L-band Digital Aeronautical Communications System
LDACS-NAV	LDACS, um Navigationskomponente erweitert

LEO	Low Earth Orbit
LORAN	Long Range Navigation System
MAGNAV	Magnetfeldnavigation
MLP	Multi-Layer Perceptron
NATO	North Atlantic Treaty Organization
NAVSTAR GPS	Navigation Signal Timing and Ranging Global Positioning System
NAVWAR	Navigation Warfare
OSNMA	Open Service Navigation Message Authentication
P-Code	Precision-Code
PRN-Code	Pseudorandom Noise-Code
PNT	Positionierung, Navigation und Zeitbestimmung (PNZ), engl. positioning, navigation and timing
PPS	Precise Positioning Service
PRS	Public Regulated Service
Pseudolite	Pseudo Satellite
P(Y)-Code	verschlüsselter P-Code
PSE	Pseudoentfernung
R-Mode	Ranging Mode
RAIM	Empfängerautonome Integritätsprüfung (engl. Receiver Autonomous Integrity Monitoring)
RNSS	Radio Navigation Satellite Service
RTK	real-time kinematic
SA	Selective Availability
SBAS	satellitenbasierten Ergänzungssystemen (engl. Satellite Based Augmentation System)
SPS	Standard Positioning Service
STFT	Short-Time-Fourier-Transformation
TAWS	Terrain Awareness and Warning Systems
TACAN	TACTical Air Navigation
UAV	unbemannte Luftfahrzeuge (engl. unmanned aerial vehicle)
UWB	Ultra-WideBand
UTC	koordinierte Weltzeit (engl. Universal Time Coordinated)
WAAS	Wide Area Augmentation System
ZGeoBw	Zentrum für Geoinformationswesen der Bundeswehr

1 Einleitung

„Wenn Sie nicht wissen, wo Sie sind, sind Sie eigentlich tot!“

Dieses Zitat stammt aus der Vorlesung „Geoinformatik“ vom 10.10.2023 von Professor Roland Wagner an der Berliner Hochschule für Technik. Er äußerte dieses Zitat im Kontext der Navigation von Flugzeugen. Früher sei es üblich gewesen, dass drei Menschen im Cockpit saßen, wovon einer als Navigator fungierte und sich um nichts anderes gekümmert hat als die Position zu bestimmen (WAGNER 2023). Das Zitat bringt die essenzielle Bedeutung präziser Standortbestimmung und der Kenntnis des eigenen Standortes auf den Punkt.

In einer zunehmend vernetzten und automatisierten Welt sind verlässliche Positionsdaten für zahlreiche zivile und militärische Anwendungen unerlässlich. Doch genau diese Abhängigkeit macht globale Navigationssatellitensysteme (GNSS) anfällig für gezielte Störungen. Zwei der relevantesten Bedrohungen sind Jamming, die absichtliche Überlagerung des GNSS-Signals durch stärkere Störsignale, und Spoofing, die Täuschung durch gefälschte Satellitensignale.

Das Thema Jamming gewinnt zunehmend an Bedeutung, egal welchen Anwendungsbereich man sich anschaut. Sei es wie hier in der Arbeit behandelt im Bereich der Nutzung von GNSS-Systemen, aber auch im Bereich Kommunikation, dies sowohl in militärischen als auch zivilen Zusammenhängen (ROOPER 2019). Im militärischen Einsatz wird die weltraumgestützte Fähigkeit immer essenzieller, diese liefert Daten, Produkte und Dienste für Positionierung, Navigation und Zeitbestimmung (PNZ, engl. positioning, navigation and timing (PNT)) (NÖTZOLD 2024). Mit zunehmender Nutzung von GNSS steigt jedoch die Gefahr gezielter Signalstörung. Beispielsweise werden in der (zivilen) Luftfahrt und im militärischen Einsatz von unbemannten Luftfahrzeugen (engl. unmanned aerial vehicle, UAV) häufiger Störungen beobachtet, unter anderem vermehrt seit Beginn der russischen Invasion auf die Ukraine (NAGY 2024). Neben dem Jamming gibt es auch noch das Spoofing. Spoofing bezeichnet, das gezielte Aussenden falscher Koordinaten gesendet, um die Position zu fälschen, beispielsweise wie bei den Öltankern, die trotz Sanktionen im Rahmen der russischen Invasion gegenüber Russland an der russischen Küste zum Laden angelegt haben (TRIEBERT et al. 2023).

Vor diesem Hintergrund wurde die vorliegende Arbeit verfasst, um einen aktuellen und umfassenden Überblick über die Auswirkungen von GNSS-Störungen durch Jamming und Spoofing sowohl zivil und militärisch als auch in der Unterteilung in maritime, luft- und bodengestützte Anwendungen zu geben. Zudem werden die Erkennungen solcher Störungen, wirksame Gegenmaßnahmen sowie mögliche alternative Navigationsverfahren untersucht und kritisch bewertet. Damit leistet die Arbeit einen Beitrag zum besseren Verständnis der Verwundbarkeit moderner PNT-Systeme und zeigt Wege zur Erhöhung der Resilienz auf.

Die Aktualität des Themenbereiches kann in den aktuellen Konfliktregionen, wie dem Russland-Ukraine-Krieg, aber auch dem brandaktuellen Konflikt im Bereich Israel-Iran, nachvollzogen werden. Die unterschiedlichen Konfliktparteien, sei es direkt oder indirekt, nutzen in Rahmen der sogenannten Navigation Warfare (NAVWAR) gezielt GNSS-Jamming und Spoofing. Die aktuellen Auswirkungen (Stand: Juni 2025) werden anhand eines Beispiels einer Website, die Jamming und Spoofing auf Flugzeuge zeigt, dargelegt (SKAI DATA SERVICES 2025). Die zunehmende geopolitische Instrumentalisierung von Navigationsstörungen verdeutlicht, dass GNSS längst mehr als nur ein technisches Hilfsmittel ist, sondern ein sicherheitspolitisch relevantes Schlüsselement.

Die Arbeit gliedert sich neben der Einleitung, den Inhalts-, Abbildungs-, Formel-, Tabellen-, Abkürzungs- und Literaturverzeichnissen und dem Ausblick in vier Hauptkapitel. Kapitel 2 beginnt mit einem Überblick über die Funktionsweise und eine Auswahl an Anwendungsfelder von GNSS gegeben. Im Anschluss daran wird auf mögliche Störungen von GNSS-Signalen eingegangen, hier besonders auf die Störungsquellen Jamming und Spoofing und deren Anwendung im zivilen und militärischen Kontext. Im vierten Kapitel werden mögliche Auswirkungen auf zivile und militärische, sowie maritime, luft- und bodengestützte Anwendungen anhand von Beispielen, wie oben bereits angeschnitten, erläutert. Das Störungsmanagement von Jamming und Spoofing in Form von Detektion, Gegenmaßnahmen sowie alternative Navigationsverfahren wird im fünften Kapitel beschrieben. In allen Kapiteln wird sowohl auf militärische als auf zivile Anwendungsbereiche eingegangen.

2 GNSS

In der heutigen Welt basieren zahlreiche Systeme auf PNT-Bestimmung, sei es in Fahrzeugen, Flugzeugen, Navigationsapps auf Smartphones oder in der modernen Landwirtschaft (Automatisierung) (MANSFELD 2010). Jeder ist, auch wenn unbewusst, auf die Nutzung von GNSS angewiesen. Im folgenden Kapitel werden die Grundlagen und mögliche Anwendungsfelder von GNSS beschrieben. In den GNSS-Grundlagen wird aufgrund der Kürze der Arbeit nur der für das Thema Störung von GNSS relevante Ausschnitt dargestellt.

2.1 GNSS-Grundlagen

Die aktuellen Navigationssatellitensysteme, welche zur Bestimmung von Position, Geschwindigkeit und Zeit verwendet werden können, bestehen aus vier globalen und zusätzlichen regionalen Navigationssystemen (BAUER 2017). Das bekannteste GNSS ist das amerikanische „Navigation Signal Timing and Ranging Global Positioning System“ (NAVSTAR GPS), welches umgangssprachlich GPS genannt wird. Viele Anwender nutzen diesen Begriff, wenn sie GNSS im Allgemeinen meinen (MANSFELD 2010). Ein solcher GPS-Satellit ist in der Abbildung 2-1 zu sehen. Weitere GNSS sind das russische



Abb. 2-1: GPS III SV01 Satellit (LOCKHEED 2019)

„GLObalnaya NAVigatsionnaya Sputnikovaya Sistema“ (GLONASS), das europäische Galileo System sowie das chinesische BeiDou System (BDS) (LUBER 2025). Die GNSS bestehen aus dem Raum-, Kontroll- und Bodensegment, zur genaueren Erklärung der einzelnen Systeme und Segmente wird auf LUBER (2025) und BAUER (2017) verwiesen.

Zur Positionsbestimmung eines Empfängers von Satellitensignalen müssen mindestens vier Satelliten zur Verfügung stehen (LUBER 2025). Bei der Positionsbestimmung mittels GNSS wird in drei Beobachtungsgrößen zur Berechnung unterschieden. Diese lauten Pseudoentfernung aus Code-Messung, Entfernung aus Trägerphasenmessung und Doppler-Frequenzverschiebung (MANSFELD 2010). Bei der Bestimmung der Position mittels Pseudoentfernung *PSE* werden vom Empfänger die Signale empfangen und daraus die Entfernungen zum Satelliten berechnet. Diese Berechnung erfolgt, wie in Formel 2-1, zusehen durch die Multiplikation der Laufzeitdifferenz Δt mit der Lichtgeschwindigkeit c (BAUER 2017,

MANSFELD 2010). Die Pseudostrecke unterscheidet sich von der tatsächlichen Entfernung aufgrund von Einflussgrößen, wie Ausbreitung des Signals und Uhrenfehlern. Auf mögliche Einflüsse wird im Laufe des Kapitels eingegangen. Für die Laufzeitdifferenz erzeugt der Empfänger eine Codesignalnachbildung zum nominal gleichen Zeitpunkt wie der Satellit. Die Laufzeitdifferenz ist der Unterschied zwischen der Referenzzeit des Empfängers zum Zeitpunkt des Signalempfangs und dem Zeitstempel aus dem ausgesendeten Signal. Es erfolgt also eine Bestimmung aufgrund der Laufzeit des Signales anhand der Korrelation des Pseudorandom Noise-Codes (PRN-Code) (MANSFELD 2010). Die Erklärung zum PRN-Code befindet sich weiter hinten in diesem Kapitel. Zur Bestimmung der PSE wird die GNSS-Zeit vorausgesetzt. Diese wird laut JEKELI et al. (2017) für jedes GNSS mittels eigener Zeitsysteme, welche über satelliteninterne Atomuhren und die SI-Sekunde¹ definiert werden, bestimmt. Außerdem werden diese GNSS-Zeiten zusätzlich in anderen Systemen zur sehr präzisen Zeitbestimmung eingesetzt. Die GNSS-Zeiten weisen zur koordinierten Weltzeit (engl. Universal Time Coordinated, UTC) Differenzen auf (JEKELI et al. 2017).

$$PSE = c * \Delta t$$

Formel 2-1: Pseudoentfernung (nach MANSFELD 2010)

Die Bestimmung der Strecke mittels Trägerphasenmessung ist genauer als die der Laufzeitmessung. Laut BAUER (2017) und MANSFELD (2010) wird bei der Trägerphasenmessung (siehe Formel 2-2) mithilfe der Phasendifferenz $\Delta\phi$, zwischen dem empfangenen und lokal erzeugten Signal, der Laufwegunterschied in Bruchteilen einer Wellenlänge λ bestimmt. Zusätzlich zur Phasendifferenz muss die Mehrdeutigkeit N ermittelt werden. Sie entsteht aus der Anzahl der ganzen Phasenzyklen des Signals. Diese müssen bestimmt werden, da sich die Trägerphase ϕ_T im Abstand einer Wellenlänge wiederholt und somit das Ergebnis der Phasendifferenz nicht eindeutig ist (BAUER 2017, MANSFELD 2010). Aufgrund der Komplexität und Tiefe dieser Bestimmung, wird hier auf eine genauere Erklärung verzichtet, als ausführliche Erläuterung wird auf BAUER (2017) verwiesen. Außerdem wird die Wellenlänge des Signals zur Berechnung der Entfernung benötigt. Da bei der Nutzung von GNSS sich sowohl der Sender (Satellit) als auch der Empfänger bewegen, kommt es zu einer sich ändernden Entfernung. Das Referenzsignal im Empfänger und GNSS-Signal, das den Empfänger erreicht, haben nur bei konstanter Entfernung die gleiche Frequenz (MANSFELD 2010). Da die Sender und Empfänger eine Relativgeschwindigkeit zueinander aufweisen, entsteht die Doppler-Frequenzverschiebung.

$$\phi_T \cdot \lambda = (\Delta\phi + N) \cdot \lambda$$

Formel 2-2: Strecke aus Trägerphasenmessung (BLUM 2022)

¹ Definition: 9.192.631.770-mal die Periode der ausgesandten Strahlung, die dem Übergang zwischen zwei hyperfeinen Energieniveaus des Grundzustandes des Cäsium-133-Atoms entspricht (BAUER 2017)

Es gibt zwei Grundprinzipien der GNSS-Ortung, diese werden in absolute und differenzielle Ortung unterschieden. Ortung bezeichnet allgemein das Bestimmen des Standortes eines Objektes oder einer Person, während die Positionsbestimmung die genaue Ermittlung geografischer Koordinaten umfasst. Die absolute Ortung liefert die Position, Geschwindigkeit und Zeitinformationen (BAUER 2017). Zur Bestimmung der metergenauen Position wird der räumliche Pythagoras verwendet, zusätzlich muss der Uhrenfehler zwischen Satelliten- und Empfängeruhr berücksichtigt werden (MANSFELD 2010). Da für den räumlichen Pythagoras drei Unbekannte und für den Uhrenfehler eine Unbekannte entstehen, werden zur Positionsbestimmung die PSE zu vier Satelliten benötigt (BLUM 2022). Genauer als die absolute Ortung ist die differenzielle Ortung, welche für das System GPS differentiell GPS (DGPS) genannt wird. Hierbei werden wie in Abbildung 2-2 zu sehen zwei Empfänger verwendet. Laut SCHÜTTLER (2022) fungiert einer als Referenzempfänger und berechnet dauerhaft seine absolute Position. Der zweite Empfänger, der sogenannte Rover, korrigiert seine absolute Position anhand der Position des Referenzempfängers. Dafür muss eine geringe Entfernung zwischen beiden Empfängern bestehen. Dieses Verfahren liefert GNSS-Genauigkeiten im Millimeterbereich, da die unzureichend bekannte Ausbreitungsgeschwindigkeit der Satellitensignale und die unzureichenden Informationen zu Bahndaten bei beiden Empfängern gleich sind, können diese eliminiert werden und es erfolgt eine Verbesserung der absoluten Position (SCHÜTTLER 2022, BAUER 2017).

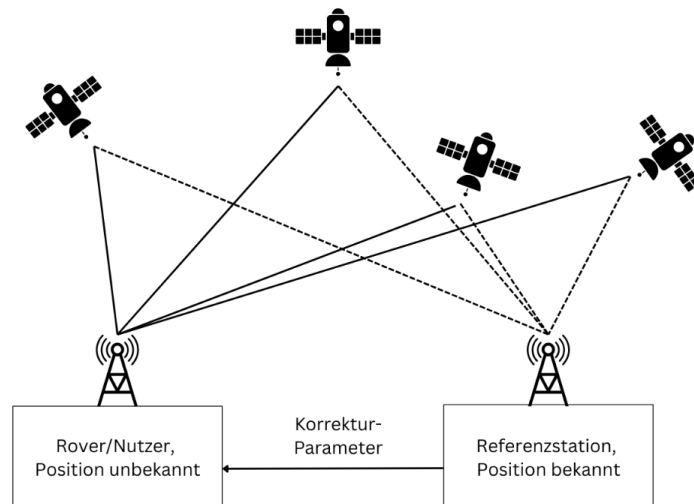


Abb. 2-2: Prinzip von Differentiellem GPS (erstellt nach SCHÜTTLER 2022)

Das Signal des Satelliten besteht aus einem Trägersignal, einem Codesignal und einem Datensignal. Die bestimmte Frequenz, auf der das Trägersignal erzeugt wird, wird Trägerfrequenz genannt (MANSFELD 2010). Das Datensignal besteht aus einer Navigationsnachricht in Bits, die Inhalte wie Ephemeridendaten und Zeitinformationen enthält. Ephemeridendaten sind die Satellitenbahndaten (BAUER 2017). Der genau Aufbau dieser Daten sowie der Aufbau der Navigationsnachricht kann in BAUER (2017) und MANSFELD (2010) nachgelesen werden.

Das Codesignal besteht aus dem PRN-Code, welcher eine Binärfolge darstellt. Die Trägerfrequenz wird mittels Phasenmodulation über den PRN-Code moduliert (BAUER 2017). Jeder GPS-Satellit sendet einen eigenen PRN-Code aus, dies ermöglicht eine fehlerfreie Zuordnung. Dies gilt ebenfalls für Galileo und BeiDou, GLONASS hingegen arbeitet mit leicht verschobenen Frequenzbereichen. Beim GPS gibt es zwei Genauigkeitspotentiale der Ortung, die als Ortungssignal eine codierte PRN-Impulsfolge verwenden (MANSFELD 2010). Das Standard Positioning Service (SPS) führt die Bezeichnung clear/aquisition Code (C/A-Code), ist frei verfügbar und dient für den Beginn des Messvorgangs. Der Precise Positioning Service (PPS) besitzt die Bezeichnung Precision-Code (P-Code) und ist dem Militär vorbehalten. Wird dieser P-Code verschlüsselt, heißt er P(Y)-Code (MANSFELD 2010).

Die Weiterentwicklung des P-Codes ist der Militär-Code (M-Code), dieser ermöglicht die autonome Nutzung des Signales zur Positionierung und befindet sich aktuell in der Einführung. Es wurde die Störfestigkeit in Form der Signalstruktur und der Leistung überarbeitet (MEURER 2024). Es muss nicht mehr vorher auf den C/A-Code zugegriffen werden (LUCCIO 2022). Dies bringt den großen Vorteil, dass nicht erst der öffentlich zugängliche und unter Umständen beschädigte oder gestörte Code genutzt wird und eine mögliche Fehlerquelle ausgeschlossen werden kann. Aktuell befinden sich 24 M-Code-fähige Satelliten im All (MEURER 2024). Mit der Einführung des M-Codes wurde das Sicherheitskonzept ebenfalls überarbeitet, dies beinhaltet unter anderem den Nutzern Gruppen zuzuordnen, welche selektiv den Zugang verwehrt bekommen können (MÜLLER 2008). Unter dem Begriff „Nutzer“ sind im GNSS-Kontext, sowohl Menschen als auch GNSS-fähige Systeme zu verstehen.

Um die Auswirkungen von Jamming und Spoofing auf GNSS-Empfänger, sowie mögliche Detektionsmechanismen und Gegenmaßnahmen in den folgenden Kapiteln zu verstehen, ist ein grundlegendes Verständnis der internen Signalverarbeitung im Empfänger erforderlich. Die genaueren Inhalte können in BAUER (2017) nachgelesen werden. Dieser wird zudem bei der Beschreibung des Aufbaus als Referenz genutzt. Die wesentlichen Bauteile (Abb. 2-3) sind die Antenne, der Front-End, der Basisbandprozessor und der Anwendungsprozessor.

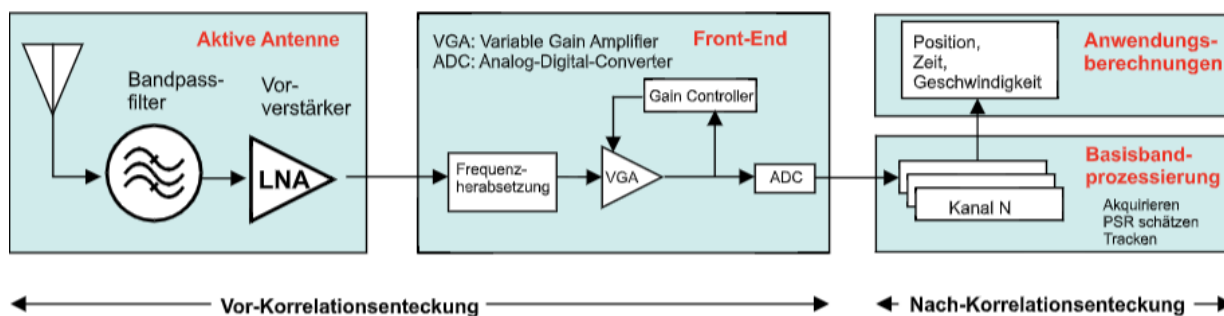


Abb. 2-3: Elemente eines GNSS-Empfängers (BAUER 2017)

Anhand der Antenne können die eingefallenen Feldstärken der GNSS-Signale in Wechselströme umgewandelt werden. Der Bandpassfilter gibt nur gewünschte Wechselströme bzw. Frequenzen zur Verarbeitung weiter. Wenn wie in diesem Fall ein Vorverstärker genutzt wird, handelt es sich um eine aktive Antenne, sonst um eine Passive. Mit dem Front-End sollen sowohl die hochfrequenten Satellitensignale auf eine deutlich niedrigere Zwischenfrequenz herabgesetzt werden als auch die Digitalisierung des Signals. Bei der Digitalisierung wird das analoge Signal mittels Analog-digital-Wandlers (engl. Analog-Digital-Converter, ADC) in digitales Signal gewandelt. Der Basisbandrechner, welcher die digitalisierten Signale erhält, akquiriert die empfangenen GNSS-Signale. Dabei analysiert er welche Satelliten von der Antenne empfangen werden und schätzt die groben Werte für die Trägerfrequenz und die Codephase jedes sichtbaren Satelliten. Jedes Signal wird einem eigenen Kanal zugewiesen, bei Mehrfrequenzempfängern auch mehrere Kanäle pro Satellit. Die Pseudostrecken werden durch Korrelation zwischen dem empfangenen Signal und einer Signalnachbildung ermittelt. Anschließend erfolgt das Tracking, bei dem dauerhaft die Signale nachverfolgt werden. Genauere Erklärungen zum Tracking und zur Basisbandprozessierung können in BAUER (2017) nachgelesen werden. Zum Schluss erfolgt die Berechnung von PNT-Informationen im Anwendungsrechner. Weitere Funktionen des Rechners sind möglich, diese zählen allerdings nicht zu den originären GNSS-Fähigkeiten.

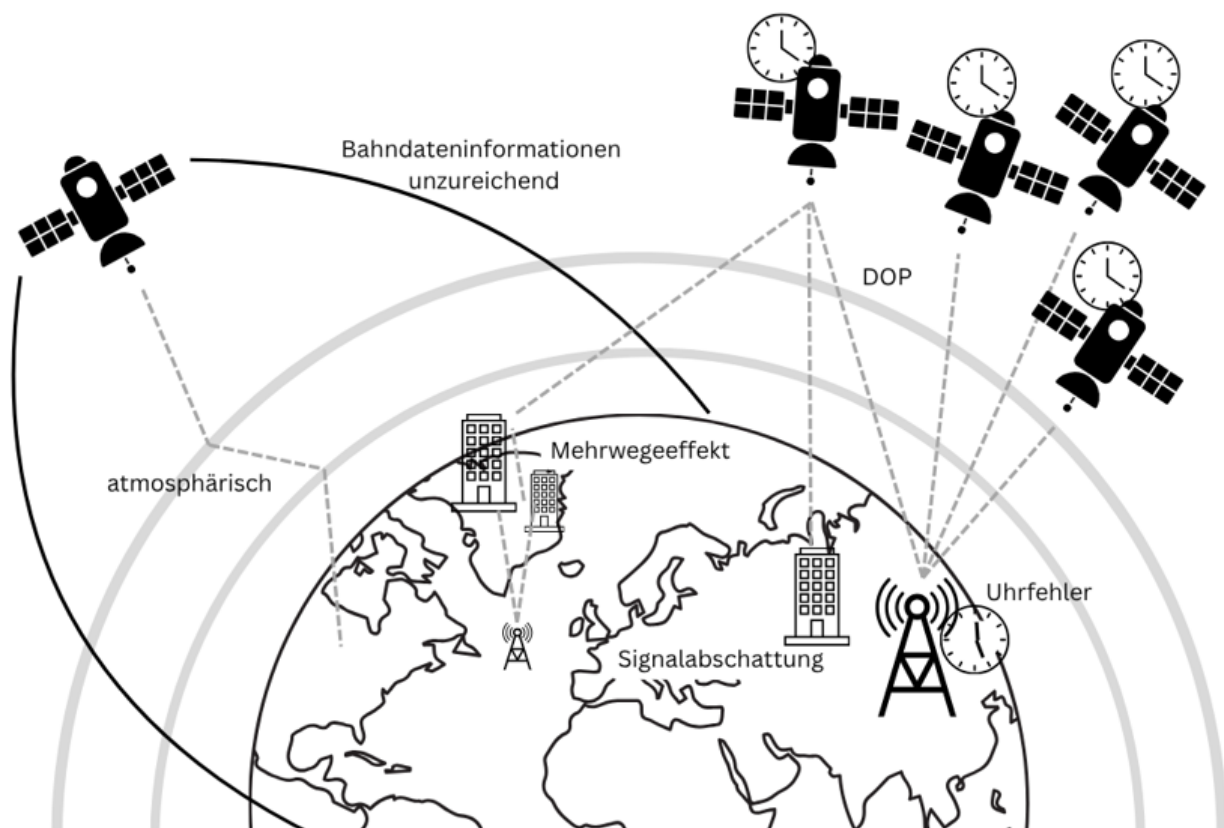


Abb. 2-4: mögliche Fehlereinflüsse auf GNSS (erstellt nach BAUER 2017, MANSFELD 2010)

Neben dem Uhrfehler des Empfängers, die unzureichend bekannte Ausbreitungsgeschwindigkeit der Satellitensignale und die unzureichenden Informationen zu Bahndaten gibt es laut MANSFELD (2010) weitere Fehlereinflüsse bei der Verwendung von GNSS. Einige der hier genannten Fehlereinflüsse werden in der Abbildung 2-4 dargestellt. Zusätzlich zu den satellitenbezogenen Fehlern, gibt es atmosphärische Fehler, wie Verzögerungen durch die Ionosphäre oder Troposphäre, signalbezogene Fehler, durch Mehrwegeausbreitung (engl. Multipath) oder Signalabschattung, und geometriebezogene Einflüsse durch ungünstige räumliche Verteilung im Raum oft durch die Dilution of Precision (DOP) ausgedrückt. Beim Multipath-Effekt kommt es zur Interferenz des direkten und reflektierten Signals. Es gibt als empfängerbezogenen Fehler nicht nur den Uhrfehler, sondern auch das Empfängerrauschen, bei dem die Genauigkeit der Code- und Phasenmessung beeinflusst wird, und die Antenne und ihre Kalibrierung. Das thermische bzw. natürliche Rauschen des Empfängers, also kleinste Stromschwankungen, die auf die Bewegung der Ladungsträger im Empfänger zurückzuführen sind, stellen ebenfalls eine Fehlerquelle da (BAUER 2017). Ein Fehler von nur einer Millisekunde kann bereits einen Positionsfehler von um die 300 km verursachen (MANSFELD 2010).

Die Signalqualität wird durch die erwähnten Fehlereinflüsse beeinflusst, sodass das GNSS-Signal nie ungestört beim Empfänger ankommt. Jedes Signal setzt sich aus einem gewollten und einem ungewollten Teil zusammen. Laut BAUER (2017) hängt die Qualität eines Signals davon ab in welchem Verhältnis die Stärke des gewollten Signals zur Stärke der Störsignale steht. Hierzu werden zwei Quotienten genutzt. Der Signal-zu-Rauschen-Quotient (engl. Signal-to-Noise Ratio, SNR), welcher aus der Signalstärke S des Empfängersignals und der Signalstärke des Störsignals N gebildet wird. Der zweite Quotient ist der Träger-zu-Rauschen-Dichte-Quotient C/N_0 (engl. Carrier to Noise Ratio), dieser wird aus der Trägerstärke des Empfangssignals C und der Spektraldichte des Störsignals pro Herz N_0 berechnet. Beide Quotienten, welche in den Formeln 2-3 und 2-4 dargestellt sind, werden nach der Korrelation des Referenzsignals und des GNSS-Signals im Empfänger ermittelt.

$$SNR = \frac{S}{N}$$

Formel 2-3: Signal-zu-Rauschen-Quotient (BAUER 2017)

$$C/N_0 = \frac{C}{N_0}$$

Formel 2-4: Träger-zu-Rauschen-Dichte-Quotient (BAUER 2017)

GNSS-Signale sind elektromagnetische Wellen im Mikrowellenbereich. Diese werden abhängig von ihrer Wellenlänge in verschiedene Frequenzbänder unterteilt. Das untere L-Band mit einer Frequenz von 1.164 MHz bis 1.300 MHz und das obere Frequenzband (1.559 MHz bis 1.610 MHz) ist den GNSS zugeordnet (BLUM 2022). Wie in der Abbildung 2-5 zu sehen, nutzen die verschiedenen GNSS unterschiedliche Frequenzen. Der Abbildung sind zwei Status zu entnehmen. Der erste Status ist der Radio Navigation Satellite Service (RNSS), welcher keinen besonderen Schutz der Signale aufweist. Der zweite Status ist der Aeronautical Radio Navigation Service (ARNS), dieser weist den Schutz auf und ist für sicherheitsempfindliche Verwendungen geeignet (BLUM 2022).

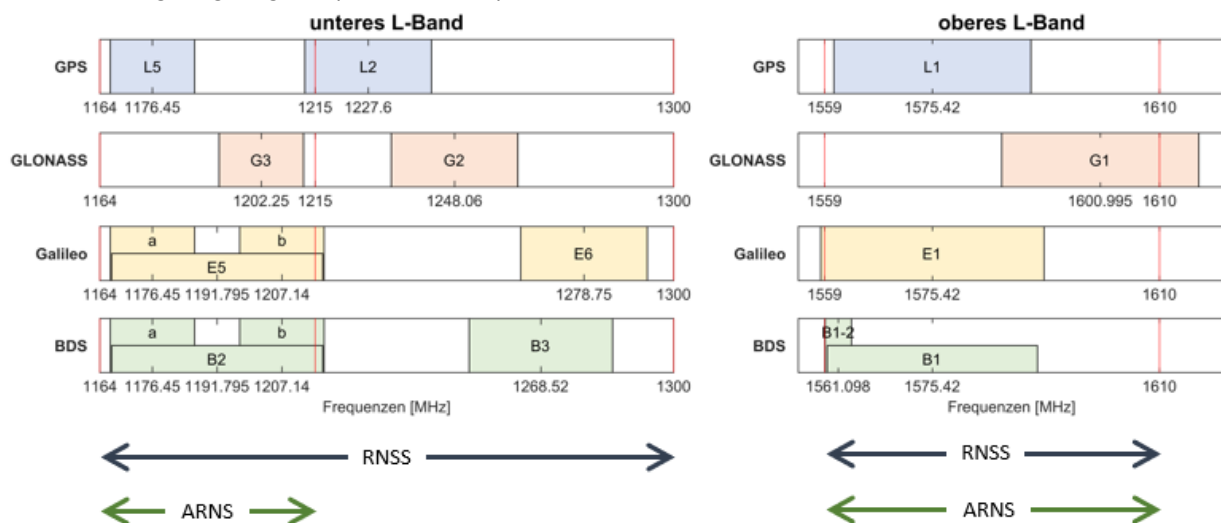


Abb. 2-5: GNSS-Frequenzbereiche in unteren und oberen L-Band (BLUM 2022)

Aufgrund dessen, dass beim GNSS sehr geringe Empfangssignalstärken verwendet werden, kann es zu Jamming und Spoofing kommen. Beim GPS zum Beispiel sendet der Satellit mit 25 W (44 dBm²) Leistung auf der zivilen L1 Frequenz (1575 MHz) und mit 4,5 W (37 dBm) auf dem militärischen L2 Frequenzband. Auf der Erde kommt eine Signalstärke von nur -136 dBm im L1-Band und -128 dBm im L2-Band an, aufgrund der Distanz von 20.000 km und den Leistungsverlusten durch die Atmosphäre. Der Wert natürlichen Rauschens liegt bei etwa -108 dBm deutlich über dem Nutzsignal von GPS. Die Verarbeitung des empfangenen Signals ist aufwendiger, sobald zusätzlich ein Störsender in diesem Frequenzbereich aktiviert wurde, der das GPS-Signal überlagert, besteht keinerlei Verbindung zwischen Satelliten und Empfänger (FINK 2013).

Die in diesem Kapitel dargelegten Eigenschaften und Schwächen der GNSS-Signale, insbesondere ihre geringe Signalstärke sowie die Vielzahl an möglichen Störeinflüssen, machen sie anfällig für gezielte Störungen in Form von Jamming und Spoofing. In den folgenden Kapiteln werden daher diese Methoden näher dargestellt.

² dBm sind ein Leistungspegel in Dezibel (dB) in Bezug auf ein Milliwatt (mW) (KULPA 2004)

2.2 Anwendungsfelder von GNSS

Die Anwendungsbereiche von GNSS sind sehr vielseitig und reichen weit über die ursprünglich militärisch motivierte Zielsetzung hinaus. Aufgrund der thematischen Breite kann im Folgenden nur ein systematischer Überblick über zentrale zivil-kommerzielle sowie sicherheitsrelevante Einsatzfelder gegeben werden. Die militärische Anwendung wird im Unterkapitel 3.3 im Zusammenhang des Jammings und Spoofings dargestellt. In den folgenden drei Unterkapiteln werden terrestrische, maritime und luftgestützte Anwendungen vorgestellt (Abb. 2-6)

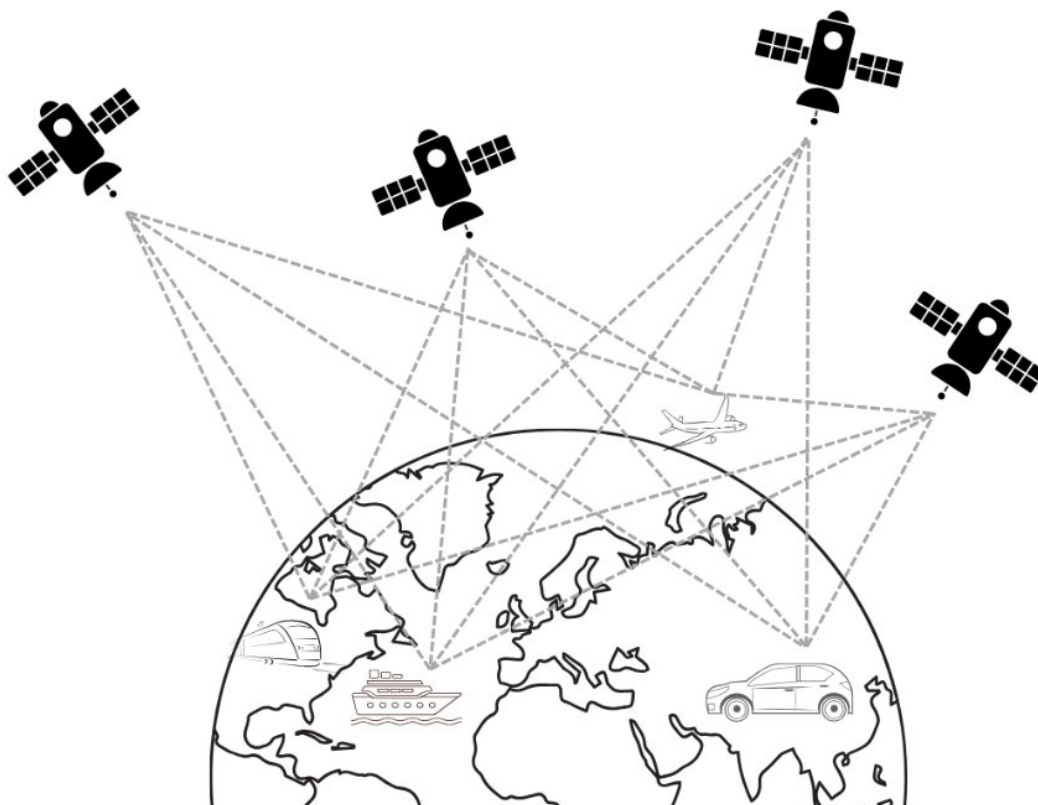


Abb. 2-6: mögliche Anwendungsbereiche (erstellt nach MANSFELD 2010)

Neben der reinen Positions- und Navigationsfunktion spielt insbesondere das „T“ für Timing eine zentrale Rolle im Begriff PNT. GNSS-Satelliten verfügen über hochpräzise Atomuhren und ermöglichen dadurch eine exakte Zeitsynchronisation. Diese ist essenziell für zahlreiche kritische Infrastrukturen, wie etwa Telekommunikationsnetze, Stromversorgungsnetze, Finanztransaktionen, das Verkehrsmanagement sowie für wirtschaftliche Hochpräzisionsanwendungen (vgl. Kapitel 4) (WESTBROOK 2019).

Unabhängig von den drei Hauptanwendungsbereichen dieses Kapitels finden sich weitere relevante Einsatzfelder unter anderem in der Raumfahrt, beim Geotagging digitaler Inhalte sowie in der Zeit- und Frequenzsynchronisation von technischen Systemen, einschließlich sicherheitskritischer Infrastrukturen (LUBER 2025).

2.2.1 Bodengestützte Anwendungen

GNSS-Systeme haben sich in den letzten Jahren zunehmend in landbasierten Bereichen etabliert, sowohl im Alltag als auch in professionellen Anwendungen. Besonders im Straßenverkehr, in der Landesvermessung und in der Landwirtschaft ergeben sich vielfältige Einsatzmöglichkeiten.

Die Wenigsten nutzen zur Navigation im Straßen-/ Landverkehr noch analoge Karten. die Nutzung von GNSS nimmt in diesem Bereich immer weiter zu, da die Positionierung und Navigation durch Technik übernommen werden. Durch solche Assistenzsysteme kann der Fahrer sich ausschließlich auf den Verkehr konzentrieren (MANSFELD 2010). Zudem kann sowohl auf der Straße als auch im Schienenverkehr der Verkehrsfluss und -ablauf erheblich verbessert werden. Verschiedene Einsatzzwecke der GNSS im Straßenverkehr sind das Zielführungssystem zum Erreichen eines gewünschten Ortes, das Positionsmeldesystem zum Beispiel für Carsharing und Transportunternehmen sowie das Verkehrsleitsystem zur Koordinierung mehrerer Fahrzeuge im ÖPNV. Der genauere Aufbau und die detaillierte Funktion dieser kann im MANSFELD (2010) und SCHÜTTLER (2022) nachgelesen werden.

In der Landesvermessung, aber auch in anderen Bereichen der Geodäsie wird ebenfalls GNSS genutzt, sei es zur Orientierung, Positionierung, aber auch als Korrekturdaten (MANSFELD 2010). In der Land- und Forstwirtschaft wird GNSS zum gesteuerten Einsatz von Bodenbearbeitungs- und Erntemaschinen sowie zur Transportlenkung beim Holzeinschlag verwendet.

Zudem kann GNSS zum Monitoring verwendet werden, zum Beispiel im Bereich Erdbeben Deformationen, Magmatismus und Oberflächenprozesse (SCHUH et al. 2017). Hier wurde die Plattentektonik im Bereich Chile observiert, um Veränderungen frühestmöglich wahrzunehmen und vor Folgen zu warnen. Da werden hochgenaue GNSS-Positionsbestimmungen mittels real-time kinematic (RTK), bei dem die bewegten Nutzungseinheiten hochgenaue Echtzeitpositionen erhalten, und precise

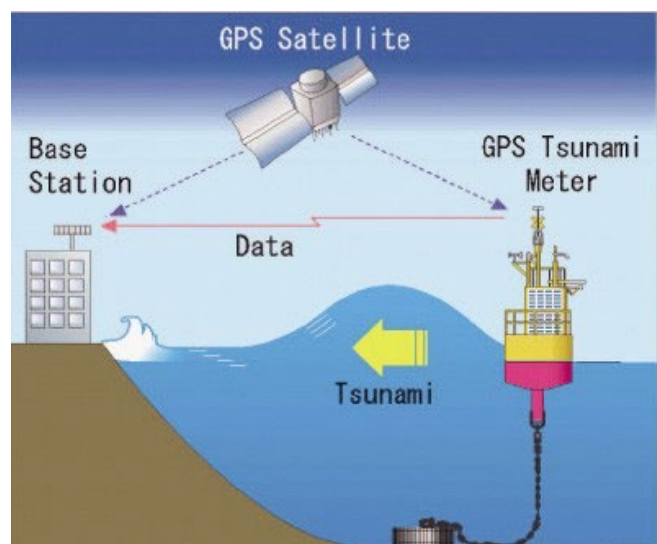


Abb. 2-7: Tsunami Warnsystem mittels GPS-Bojen
(KATO et al. 2011)

point positioning (PPP), welches ohne unmittelbar verfügbare Referenzstation hochgenaue Positionen liefert, verwendet (SCHUH et al. 2017, BAUER 2017). Außerdem wird eine Multi-GNSS-Überwachung in einem globalen Referenznetzwerk mit etwa 100 Stationen sichergestellt

(SCHUH et al. 2017). Des Weiteren können mit einem GPS-Bojensystem Tsunami-Erkennungen durchgeführt werden. Es wird, wie in Abbildung 2-7 zu sehen, RTK-GPS zusammen mit Funkübertragung und einem Internet-Verbreitungssystem eingesetzt, sodass jeder den Tsunami in Echtzeit beobachten kann (SCHUH et al. 2017). Auf jedem Smartphone wird, wenn nicht deaktiviert, ein GNSS-Signal empfangen, anhand dessen die eigene Position bestimmt und Apps für unter anderem Wettervorhersagen, Wanderungen oder Messenger-Dienste genutzt (SCHÜTTLER 2022).

2.2.2 Luftgestützte Anwendungen

Die Luftfahrt hat in der Nutzung von GNSS die höchsten Anforderungen an die Systemgenauigkeit, Zuverlässigkeit und Integrität³. Auch wenn GNSS viele Vorteile hat, ist es bisher allerdings nicht als stand-alone System zugelassen worden. GNSS wird im Streckenflug verwendet. GNSS wird nicht nur im Flugzeug verwendet, sondern auch bei zum Beispiel dem Ausbringen von Düngemitteln, der Vermessung der Erdoberfläche oder Ähnlichem mithilfe von Flugzeugen (MANSFELD 2010).

Aufgrund der unzureichenden Genauigkeit für bestimmte Flugabschnitte besonders im Zeitraum der Landung und der unzureichenden Integrität, müssen zusätzliche Systeme verbaut sein (MANSFELD 2010). Üblich ist eine Zwei- und Dreifachinstallation von Trägheitsnavigationssystemen in Kombination mit GNSS-Empfängern sowie der Einsatz zusätzlicher, auf die verschiedenen Flugabschnitte spezialisierte Funknavigationssysteme (SCHÜTTLER 2022).

Die primäre Nutzung im Landeanflug sei nicht einheitlich international geregelt, GNSS werde an deutschen Flughäfen allein verwendet, so SCHÜTTLER (2022). Um die Genauigkeit der GNSS im Bereich des Landeanfluges zusätzlich zu stärken, werden satellitenbasierte Ergänzungssysteme (engl. Satellite Based Augmentation System, SBAS) eingesetzt (BAUER 2017). Dabei handelt es sich um Systeme, welche regional begrenzt mittels geostatischer Satelliten die Zuverlässigkeit, Genauigkeit, und Verfügbarkeit der Positionsbestimmung mittels GNSS verstärken. Für den Bereich des GPS in Nordamerika ist es das Wide Area Augmentation System (WAAS) und in Europa das European Geostationary Navigation Overlay Service (EGNOS) (MANSFELD 2010). Zudem liefern diese SBAS Informationen zur Integrität des GNSS. Da diese allerdings ebenfalls von Störungen wie Jammern beeinflusst werden können, besteht trotz dessen kein vollständiger Schutz (MANSFELD 2010).

³ Korrektheit der Daten (MANSFELD 2010)

Neben SBAS existieren bodengebundene Ergänzungssysteme (engl. Ground based Augmentation System, GBAS), welche für die Verbesserung der Parameter für Landeanflüge von Flugzeugen verwendet werden. Sie verwenden ein sich auf DGPS beruhendes Verfahren und sind somit nur in Verbindung mit einem konkreten Flughafen nutzbar (MANSFELD 2010). Ein beispielhaftes Funktionsschema eines GPS-Landeanflugsystems ist in Abbildung 2-8 zu sehen. Sowohl SBAS als auch GBAS wurden primär für den Flugverkehr entwickelt, werden aber auch in Nischenbereichen genutzt.

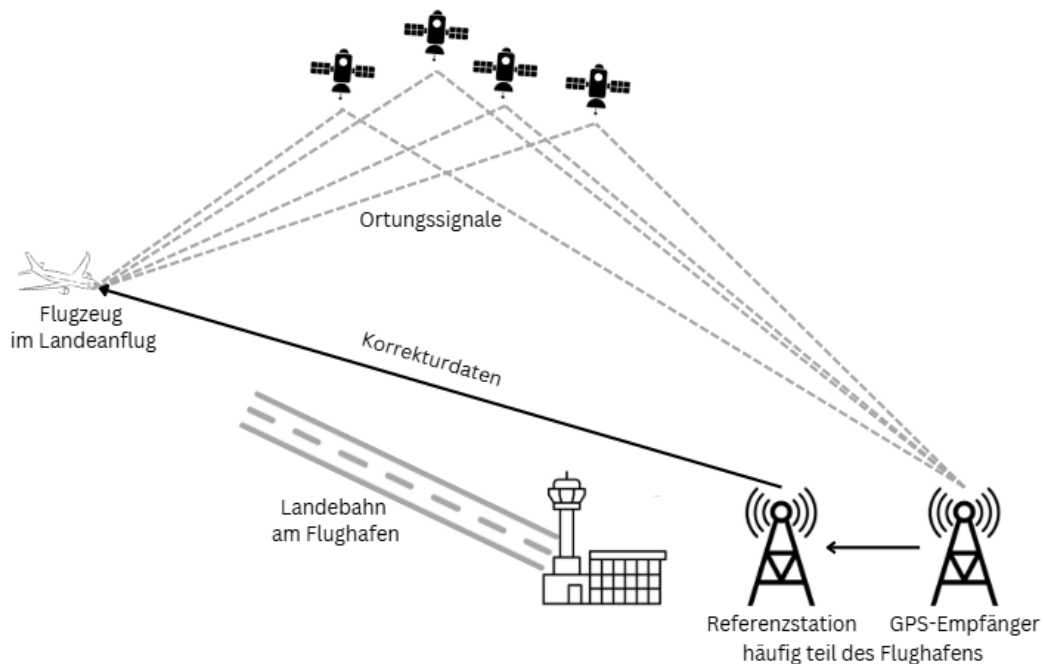


Abb. 2-8: Funktionsschema eines GPS-Landeanflugsystems (geändert nach MANSFELD 2010)

Eine weitere Möglichkeit zur Prüfung der Integrität, ist die empfängerautonome Integritätsprüfung (engl. Receiver Autonomous Integrity Monitoring, RAIM), welche sowohl in der See- als auch in der Luftfahrt verwendet wird (MANSFELD 2010). Dadurch, dass die SBAS nicht die Erde vollständig überdecken, wird dort das RAIM genutzt und als alternatives System nicht überflüssig. Da bei der Positionsbestimmung mindestens vier Satelliten benötigt werden, werden beim RAIM mindestens fünf benötigt, um Fehler auszuschließen. Je höher die Redundanz der Messinformationen, desto besser funktioniert das RAIM. Es gibt mehrere Methoden entweder werden die PSE zu den Satelliten berechnet und verglichen, die Methode der kleinsten Quadrate verwendet oder die maximale Abweichung berechnet (MANSFELD 2010). Das RAIM könnte also sowohl bei Systemfehlern des Satelliten, welche zu Signalstörungen führen, als auch bei Jamming und Spoofing verwendet werden.

GNSS wird in der Luftfahrt überwiegend in Kombination mit ergänzenden Systemen eingesetzt. Hierzu zählen satelliten- und bodengestützte Augmentationssysteme sowie empfängerautonome Verfahren zur Integritätsprüfung. Die Nutzung erfolgt anwendungs- und flugphasenabhängig unter Berücksichtigung internationaler unterschiedlich geregelter Standards.

2.2.3 Maritime Anwendungen

Auch auf und unter Wasser spielt GNSS eine zunehmend zentrale Rolle in Bereichen von der Navigation in der Seefahrt bis zur Ortung von Offshore⁴-Fahrzeugen und den Erhalt von georeferenzierten Meeresdaten. Klassische Navigationsmöglichkeiten wie optische Verfahren, funktechnische Systeme und Seekarten wurden durch die Nutzung von GNSS ersetzt, vor allem in internationalen Gewässern. In Binnengewässern müssen DGPS-Referenzstationen zur Verfügung stehen, da dort höhere Genauigkeiten benötigt werden (SCHÜTTLER 2022, MANSFELD 2010). GNSS erfüllt zum aktuellen Zeitpunkt die Anforderungen der allgemeinen Schifffahrt an Genauigkeit, Verfügbarkeit, Kontinuität und Integrität nicht (HOPPE 2017). Der GNSS-Einsatz bietet bei Such- und Rettungsaktionen einige Vorteile, wie zum Beispiel die genaue Position des Unfallortes und die einheitliche Nutzung des Koordinatensystems (MANSFELD 2010).

In der Fischerei können mithilfe von GNSS die Routen gelenkt und somit die Fischbestände geschützt werden (SCHÜTTLER 2022). Die PNT-Daten, welche das Schiff erhält, werden zusätzlich in einer Vielzahl an Bordsystemen verwendet. Die Daten werden ebenfalls mittels Automatic Identification System (AIS) an die umgebende Schifffahrt und die landseitigen Verkehrserfassungssysteme weitergegeben. Außerdem können Unfälle durch Kollisionen frühzeitig erkannt und verhindert werden (HOPPE 2017).

Zur Positionierung von Offshore-Fahrzeugen wurde relative Positionierung zweier Objekte mittels GNSS in Form des Differential Absolute and Relative Positioning Sensor (DARPS) entwickelt. Die Offshore-Fahrzeuge positionieren sich dynamisch, relativ zu anderen festen Objekten wie Windenergieanlagen. Hierbei bestimmen beide Objekte mit ihren eigenen Empfängern ihre absolute und zusätzlich ihre relative Position zueinander, darüber kann die Position des Offshore-Fahrzeuges korrigiert werden (MAJOHR et al. 2021).

Es kann mithilfe von Ultraschallsensoren die Meeresbodenstruktur abgetastet werden, um diese Daten dann zu georeferenzieren wird mithilfe von DGPS die Position bestimmt. Zusätzlich kann die Meerestiefe bestimmt werden. Dazu werden die geographischen Koordinaten und Höhe eines Flugzeuges bestimmt, sowie die Höhe zwischen Flugzeug und Meeresboden, welche durch Rückstrahlortung eines Lasers ermittelt wird. Die Höhendifferenz dieser beiden Höhen ist die Meerestiefe bezogen auf den Erdellipsoid (MANSFELD 2010). Weitere maritime Anwendungen sind in der Hydrographie zur Erstellung und Aktualisierung von Seekarten, in der Ortung und Verfolgung von Containern sowie sicherheitsrelevanten Anwendungen auf dem Schiff und im Hafen (HOPPE 2017).

⁴ engl. vor der Küste (MAJOHR 2021)

3 Störungen von GNSS-Signalen

GNSS-Systeme sind aufgrund ihrer Signalstärke im Empfangsbereich besonders störanfällig. Neben unbeabsichtigten technischen Beeinträchtigungen treten zunehmend beabsichtigte/gezielte Störungen auf. Insbesondere in sicherheitskritischen und militärischen Kontexten ist dies eine reale Bedrohung. Dieses Kapitel gibt einen Überblick über die Hauptformen von GNSS-Störungen mit dem Schwerpunkt Jamming und Spoofing. Es erläutert dessen technische Umsetzung sowie das zivile und militärische Anwendungsspektrum.

3.1 Überblick der Arten

Es gibt eine hohe Verwundbarkeit der GNSS-Signale, hierrüber schreibt BAUER (2017), welcher als Literatur für diesen und den folgenden Absatz verwendet wurde. Es gibt viele verschiedene Ursachen für Störungen, in den meisten Fällen sind es Interferenzen. Die Interferenz wird definiert als die Überlagerung der ursprünglich unbeeinträchtigten GNSS-Signale durch externe Signale oder im Fall von Multipath-Effekten durch reflektierte Anteile des eigenen Signals. Diese Überlagerungen treten auf, wenn mindestens zwei Wellenzüge, hier elektromagnetische Wellen, dasselbe Raumgebiet durchlaufen. GNSS-Interferenzen werden in zwei Gruppen gegliedert, die natürlichen und die Funkinterferenzen. Im Bereich der natürlichen Interferenzen werden die Sonneneruption und die Solarzyklusveränderung genannt. Hierbei ändert die Sonne alle 11 Jahre ihre Sonnenstrahlenintensität. Dies führt zu kurzperiodischen Schwankungen des ionosphärischen Laufzeitfehlers sowie andere Schwankungen der Signalstärke. Sind diese Veränderungen ausreichend gravierend, können die Empfänger die GNSS-Signale nicht mehr verarbeiten.

In der Kategorie der Funkinterferenzen unterscheidet BAUER (2017) in beabsichtigte (vgl. 3.2) und unbeabsichtigte (akzeptierte) Interferenzen. Die unbeabsichtigten Interferenzen können bei einer Überlappung von Frequenzbereichen verschiedener Signalquellen entstehen. Betroffen sind insbesondere die im ARNS-Band ausgestrahlten GNSS-Signale. Vor allem sind die GPS-L5 und Galileo-E5-Signale betroffen, da diese Frequenzbereiche auch durch Distance Measuring Equipment (DME) und Tactical Air Navigation (TACAN) genutzt werden. Diese beiden Systeme, welche eine starke Sendeleistung von 50 - 1000 W verwenden, sind ergänzende Navigationssysteme der Luftfahrt. Somit sind diese geeignet die Nutzung von GNSS-Signalen zu erschweren und einzuschränken.

In die Kategorie unbeabsichtigte Interferenzen fällt außerdem noch der Bereich Amateurfunk. Hier treten Unterbrechungen der Code- und Trägerphasenmessung auf. Auch wenn den Amateurfunkern das 23-cm-Band mit einer Frequenz von 1.240 – 1.300 MHz auf sekundärer Basis zugewiesen worden ist, kommt es immer wieder zu Interferenzen. Diese entstehen, da innerhalb des 23-cm-Bandes das GLONASS-G2-Signal auf der Frequenz 1.246 MHz und das

Galileo-E6-Signal bei 1.278,75 MHz liegen und sich das Band sehr dicht am, auf der Frequenz 1.227,60 MHz liegenden, GPS-L1-Signal befindet. Diese GNSS-Frequenzen sowie die Amateurfrequenz ist in Abbildung 3-1 dargestellt.

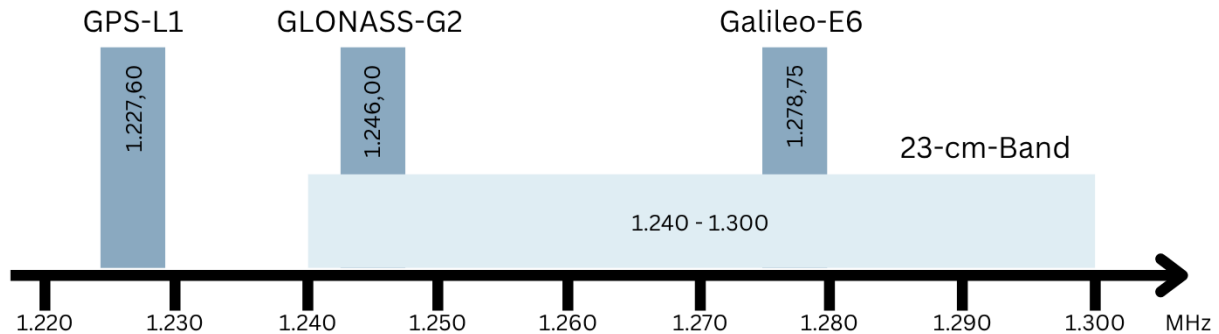


Abb. 3-1: GNSS-Signale und Amateurfunk (erstellt nach BAUER 2017)

Außerdem nimmt BAUER (2017) eine nachrichtentechnische Klassifikation der störenden Interferenzen vor. Er klassifiziert nach Frequenzbändern und Signaltypen und wird für den folgenden Absatz als Literatur verwendet. Die Klassifikation nach Frequenzbändern gliedert sich wiederum in drei verschiedene Typen. Bei der In-Band-Interferenz befinden sich die GNSS-Störsignale in den Frequenzbereichen, die auch vom GNSS-Signal genutzt werden. Diese Störsignale werden laut BAUER (2017) auch In-Band-Signale genannt. Dementsprechend ist das im vorherigen Abschnitt erwähnte GLONASS-G2-Signal ein solches In-Band-Signal. Bei den Near-Band-Interferenzen, das Nachbarband-Interferenzen genannt wird, überschneiden sich die Frequenzbänder nach der Definition von BAUER (2017) nicht. Ein Beispiel dafür ist das ebenfalls in Abbildung 3-1 dargestellte GPS-L1-Signal. Er schreibt, dass die Out-of-Band-Interferenz entsteht, in dem Moment wo das Störsignal außerhalb des GNSS-Frequenzbandes liegt. Die Entstehung dieser Out-of-Band-Störsignale erfolgt typischerweise durch eine harmonische Frequenz, also durch ganzzahlige Vielfache der Frequenz eines unterhalb des GNSS-Bandes liegenden Signals.

Bei der Klassifikation nach Signaltypen differenziert BAUER (2017) nach fünf Arten. Das Breitbandsignal (engl. Wide Band Signal) hat eine Bandbreite von 20 – 50 MHz ähnlich zur GNSS-Signalbandbreite. Das Signal mit einer deutlich kleineren Bandbreite als die des GNSS-Signals, ist das Schmalbandsignal (engl. Narrow Band Signal). Die dritte Signalart nennt sich gleichmäßige Welle (engl. Continuous Wave Signal) und ist eine reine Sinusschwingung mit gleichbleibender Frequenz und Amplitude, welche nur eine Frequenz nutzt. Ihre Bandbreite geht gegen Null und wird in der Abbildung 3-2 als Pfeil dargestellt. Zudem gibt es gepulste und Sweep-Signale. Er sagt: „ein gepulstes Signal wird mit einer bestimmten Frequenz ein- und ausgeschaltet. Die Bandbreite kann sehr unterschiedlich sein.“ Bei dem Sweep (deutsch: schweifen) Signal wird hingegen die Frequenz in einem bestimmten Intervall, welches die Signalbandbreite definiert, verändert. Eine Spezialform des Sweep-Signals ist das Chirp.

Zusätzlich zu den von BAUER (2017) genannten Arten gibt es noch das Gaußförmige Rauschen, welches Störsignale, die in Frequenz- und Zeitbereich normalverteilt sind (KONOVALTSEV et al. 2017). Diese verschlechtern die Signalqualität, da sie sich nicht vom immer herrschenden Grundrauschen (engl. Noise Floor) hervorheben und somit den Rauschpegel des Empfängers erhöhen. Außerdem gibt es laut KONOVALTSEV et al. (2017) spektral angepasste (engl. matched spectrum) Signale, bei diesen muss eine Modulation zur Erzeugung durchgeführt werden. Das Herausfiltern aus authentischen GNSS-Signalen ist aufgrund der Ähnlichkeit nicht möglich und sie können anstelle des GNSS-Signals getrackt werden und gelten somit als sehr effektive Störsignale. Einige der genannten Signalarten werden in der Abbildung 3-2 dargestellt.

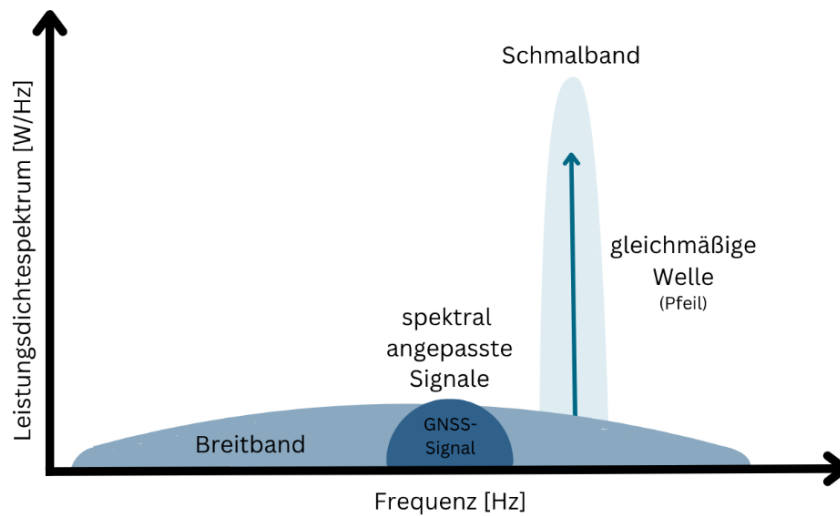


Abb. 3-2: Signalarten (geändert nach BLUM et al. 2023)

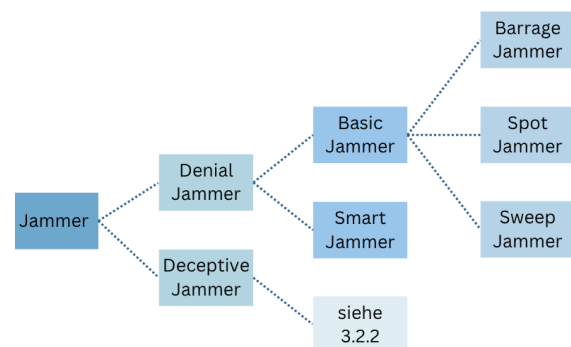
3.2 Beabsichtigte Störungen

Im Gegensatz zu den in Unterkapitel 3.1 dargestellten unbeabsichtigten Störungen, die häufig durch natürliche oder technische Fehlfunktionen entstehen, handelt es sich bei beabsichtigten Störungen um gezielte Maßnahmen zur Beeinträchtigung oder Täuschung von GNSS-Signalen. Diese absichtlichen Eingriffe stellen eine besonders ernstzunehmende Bedrohung für sicherheits- und zeitkritische Anwendungen dar, da sie meist mit strategischer Absicht erfolgen und erhebliche Auswirkungen auf PNT-Systeme haben können. Die folgenden beiden Unterkapitel konzentrieren sich auf die beabsichtigte Interferenz das Jamming und die GNSS-Störung des Spoofings.

3.2.1 Jamming

Unter Jamming versteht man laut BAUER (2017) die beabsichtigte Herbeiführung von Interferenzen. WESTBROOK (2019) schreibt: „Jamming wird verursacht durch die Übertragung eines Störsignals über eine oder mehrere GNSS-Frequenzen, um den Rauschpegel zu erhöhen oder die Empfängerschaltung zu überlasten und so den Signalempfang zu stören.“ Die dazugehörigen Störsender, welche auf den GNSS-Frequenzen Signale senden und so die GNSS-Signal Verarbeitung verhindern, werden Jammer genannt (BAUER 2017). Je stärker das Störsignal, desto eher entstehen diese Interferenzen (BAUER 2017). Neben der im folgenden Absatz beschriebenen Unterscheidung der Jammer können diese auch in weitere Kategorien differenziert werden. Die zivile sowie militärische Unterscheidung findet im Unterkapitel 3.3 statt.

Die NATO unterscheidet in zwei Jammer-Klassen, siehe Abbildung 3-3 (MEURER 2024). Es wird in den Denial Jammer, also den Störer, und den Deceptive Jammer, den Täuscher, differenziert (MEURER 2024). Da zur Klasse des Täuschers der Themenblock Spoofing gehört, wird dies in Unterkapitel 3.2.2 näher erläutert.



Es gibt laut KO (2010) und MERUER (2024) verschiedene Arten der Denial Jammer, dazu

MEURER 2024)

zählt der Basic und smart Jammer. Der Basic Jammer, wozu das Barrage, Spot, und Sweep Jamming gehört, stört unter anderem mittels Continuous Wave-, Rausch-, Puls- und Sweep Signale. Das Barrage Jamming, welches eine Breitbandstörung hervorruft, hat eine hohe Wirksamkeit gegen viele GNSS-Systeme. Die punktuelle Störung, Spot Jammer genannt, ist lediglich effektiv bei bekannter Zielnutzung und wenn deren Kanal bekannt ist. Beim Sweep Jamming, also der Durchlaufstörung, wird ein schmalbandiges Störsignal gesendet, welches kontinuierlich über das GNSS-Band läuft. Ein Nachteil dabei ist, dass die Frequenz nur kurz

gestört wird und so gegebenenfalls GNSS-Signale zwischendurch empfangen werden können. Der Smart Jammer, also die zielgerichtete GNSS-Störung, nutzt hingegen matched spectrum-Signale (KO 2010).

Die Beschreibung des Denial Jammings erfolgt auf Grundlage der Literatur von MEURER (2024). Das Ziel der Denial Jammer ist es den Empfang sowie die Auswertung von GNSS-Signalen zu verhindern. Hier gibt es zwei Ansatzpunkte. Zum einen soll das Tracking der Satelliten unterbrochen werden, zum anderen soll die Reakquisition verhindert werden. Reakquisition ist der Prozess, bei dem ein GNSS-Empfänger ein zuvor verlorenes GNSS-Signal erneut erkennt und verfolgt. Die Störwirkung ist abhängig von der empfangenen Störleistung, der Signalleistung, der spektralen Leistungsdichte des Störsenders und dem Empfängertypen.

Eine wichtige Kenngröße zur Klassifizierung des Jammers ist das Jamming-to-signal ratio (J/S) (FERRARA 2025). Dieses gibt das Verhältnis der beiden auf den Empfänger wirkenden Signale an. Das „J“ in diesem Verhältnis steht für das Störsignal und das „S“ steht für das satellitengesendete GNSS-Signal. Diese J/S-Verhältnis ist also ein Indikator dafür, ob das Störsignal stark genug ist, um das GNSS-Signal zu überlagern oder nicht. Laut SCHMIDT (2013) ist GPS besonders anfällig für Jamming in der Erfassungsphase des C/A-Codes, in dieser Phase liegt das J/S Verhältnis bei ungefähr – 27 dB, das heißt ein kostengünstiger Jammer mit einer effektiven Strahlungsleistung (engl. Equivalent Isotropic Radiated Power, ERP) von 1-Watt kann die Erfassung auf 100 km stören und die Erfassung des C/A-Codes verhindern. Der militärische Umgang mit diesem Problem wird anhand von Marschflugkörpern in Unterkapitel 3.2.4 erklärt. Laut KO (2010) sind die tolerierbaren J/S-Werte für Breitband-Störungen bei allen Signalarten (L1 C/A, P(Y), L1M) höher als bei Schmalband-Störungen.

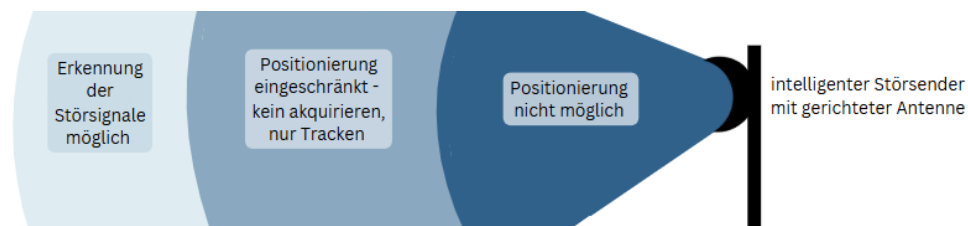


Abb. 3-4: Beeinflussung der Positionsbestimmung durch Jammer (erstellt nach MANSFELD 2010)

Jammer variieren in ihrer Leistung und Kapazität je nach Einsatzgebiet (WESTBROOK 2019), dementsprechend variiert auch der Einfluss eines Jammers auf einen GNSS-Empfänger. In der Abbildung 3-4, welche auf Grundlage von MANSFELD (2010) erstellt wurde, ist der Einfluss eines Jammers auf verschiedene Distanzen verdeutlicht. In unmittelbarer Nähe zum Störsender ist der Empfänger typischerweise nicht in der Lage, GNSS-Signale zu verfolgen, was zu einem vollständigen Verlust der PNT-Informationen führt. Mit zunehmender Entfernung kann die Signalverfolgung zwar eingeschränkt bleiben, eine grobe Positionsbestimmung ist dennoch möglich, während eine Akquisition gestört bleibt. In großer Distanz lässt sich die Präsenz eines Störsignals detektieren, ohne dass dieses die Positionsgenauigkeit merklich beeinträchtigt

(MANSFELD 2020). Diese Effekte, welche auf die verschiedenen Distanzen dargestellt sind, lassen sich ebenfalls auf verschiedene J/S-Verhältnisse übertragen. Ist das Störsignal größer als das Nutzsignal, so wird die Positionierung unmöglich. Bei einem deutlich größeren Nutzsignal ist eine Positionierung möglich und das Störsignal wird erkannt (FERRARA 2025).

Laut SCHMIDT (2013) kann es zudem ohne absichtliche Störung oder durch Jamming zu einem erhöhten J/S kommen. Dies geschieht zum Beispiel durch Abschattung mittels Bäume oder Gebäuden, aber auch die Ausrichtung der Antenne kann dies verursachen (SCHMIDT 2013). Daraus lässt sich schließen, dass das J/S-Verhältnis keinen eindeutigen Indikator für die Detektion von Jammern (vgl. 5.1) darstellt. In Unterkapitel 3.1 wurde bereits das Anti-Spoofing erwähnt, äquivalent dazu gibt es das Anti-Jamming (A/J). Es wird verwendet oder ist dazu bestimmt elektronische Störungen zu verhindern oder zu unterbinden, dazu gehören Gegenmaßnahmen (vgl. 5.2). Dieses Modul wird in Empfängern eingesetzt, um vor Jamming zu schützen (SCHMIDT 2013). SCHMIDT (2013) geht außerdem auf eine Diskussion ein, was effektiver ist, entweder ein hochleistungsfähiger Empfänger mit integrierten A/J oder ein hochpräzises inertiales Navigationssystem (INS)⁵. Zusammenfassend lässt sich sagen, dass es je nach Missionsart, Kosten-Nutzen-Verhältnis und der jeweiligen Jamming-Situation variiert.

Es betreiberintegrierte Störgegenmaßnahmen, dabei werden ebenfalls die Signale bewusst beeinflusst. Eine ist die bereits in Unterkapitel 2.1 beschriebene Verschlüsselung des P-Codes, welche auch Anti-Spoofing (AS) genannt wird. Damit versucht der Betreiber Spoofing-Angriffe, welche im Unterkapitel 3.2.2 definiert werden, zu verhindern (MANSFELD 2010). Eine weitere stellt das Flex Power da, dies bezeichnet die flexible Anpassung der Sendeleistung von Satelliten, um Störungen zu minimieren (ZHANG et al. 2025). Teilweise werden Hochspannungsleitungen als Störer aufgeführt, ob diese wirklich als Störer zu kategorisieren sind ist allerdings umstritten. Es gibt sowohl die Störung durch Abschirmung als auch die durch elektromagnetische Wellen, ob es hierbei allerdings einen signifikanten Einfluss gibt, wird diskutiert. Die genaue Argumentation ist in BLUM (2022) zu finden. Allgemein zeigen Forschungen, dass in ländlichen Regionen der GNSS-Empfang größtenteils frei von Interferenzquellen ist und in städtischen Gebieten eher Störungsquellen detektiert werden (HUMPHREY 2017).

Eine weitere zwar seltene Störungsquelle ist der Systemausfall, dieser kann entweder ein technisches Problem oder Betreiber gemacht sein (MÜLLER 2008). Zusätzliche vom Betreiber hervorgerufene Einschränkungen des Signals sind möglich. Ein Beispiel ist die Selective Availability (SA), hierbei verfügen autorisierte Nutzer über eine hohe Genauigkeit der Positionsbestimmung und für nicht autorisierte Nutzer kann die Genauigkeit willkürlich und

⁵ Kombination aus Beschleunigungsmesser und Drehratensensoren (BAUER 2017) (vgl. 5.3.1)

selektiv eingeschränkt werden (MANSFELD 2010). Die Funktionsweise von SA wurde durch eine manipulierte ausgesendete Navigationsmitteilung mit Daten zu Ephemeriden und der Uhrzeit der Satelliten definiert. Diese Art der Verfälschung wurde bei der Freigabe des GPS-Signals aus Sicherheitsgründen ins System integriert, ist allerdings seit 2000 eingestellt worden (MANSFELD 2010). Die Verbesserung der Positionierungsgenauigkeit des SPS am 02.05.2000 ist in Abbildung 3-5 zu sehen. Die vorherige Positionsgenauigkeit in der Lage verbessert sich von schlechtesten Falles 160m vertikalen Fehler und 80m horizontal zu maximal 5m. Laut MÜLLER (2008) entschied man sich neben den Vorteilen für die zivilen bzw. nicht autorisierten Nutzer auch für die Abschaltung auf Grund der operativen Handlungsfreiheit der militärischen Führung im Einsatzraum, damit diese eigenständig mit gezielter Signal-Störung reagieren kann.

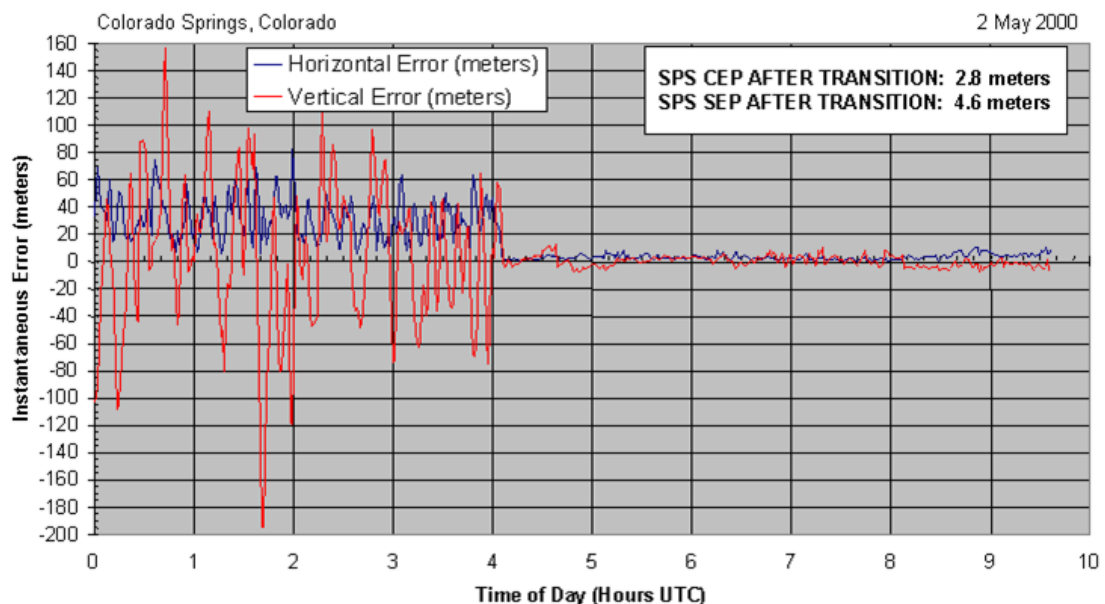


Abb. 3-5: Abschaltung der SA am 02.05.2000 (geändert nach SOKOLOV 2020)

Im folgenden Abschnitt wird ein kurzer Überblick über die historische Entwicklung des Jammings anhand der Studie von WESTBROOK (2019) gegeben. Seit dem späten 19. Jahrhundert wurde Jamming im Bereich der Radiowelle erstmals verwendet. Das Radio-Jamming spielte sowohl im Krieg als auch zu konventionellen Zwecken eine Rolle. Durch die Nutzung von Kommunikationssatelliten wurden die Auswirkungen des Radio-Jammings immer präsenter. Für die Entwicklung von neuen Jamming-Technologien waren die Einführung des GPS (1970er) und die Miniaturisierung der GPS-Empfänger in den 1980er Jahren ausschlaggebend. Durch die militärische Anwendung von GPS-Zielsystemen nahm im Laufe der beiden Golfkriege die Bedeutung und Vielseitigkeit von GPS und somit vom GPS-Jamming in der modernen Kriegsführung zu. Auslöser für die Erforschung von AS und A/J-Technologien, sowie von Technologien zur Lokalisation von Störsendern, waren russische Störsender, welche im zweiten Golfkrieg durch die irakischen Streitkräfte verwendet wurden. Die Wirksamkeit dieser ist hingegen umstritten, trotz dessen folgten Rüstungsmaßnahmen im Bereich GPS-Jamming.

Durch die Entwicklung der zusätzlichen globalen und regionalen Navigationssatellitensysteme entwickelte sich der Bereich Jamming, aber auch das Spoofing immer zügiger voran. Zusammengefasst kann man sagen, dass sich die Jamming-Technologie von der reinen Kommunikationsstörung zu einem Mittel entwickelt hat, dass die Zielgenauigkeit, Aufklärungsfähigkeit und Navigationszuverlässigkeit beeinträchtigt und dessen Relevanz sich nicht nur in der Vergangenheit entwickelt hat, sondern auch in der Zukunft weiter steigern wird.

3.2.2 Spoofing

Neben der beabsichtigten Störungsquelle dem Jamming, gibt es wie erwähnt eine zweite menschengemachte Störung, welche Spoofing genannt wird. Diese wird im folgenden Kapitel charakterisiert und die Unterscheide zum Jamming dargestellt.

Die Manipulation von GNSS-Signalen ist kein neues Phänomen, doch mit dem Aufkommen präziser Technologien hat Spoofing eine neue Relevanz erhalten. Anders als beim Jamming nutzt Spoofing die Schwächen in der Signalverarbeitung aus, um gezielt Fehlinformationen zu platzieren. WESTBROOK (2019) definiert Spoofing als die Handlung, eine gefälschte Version von GPS-Signalen, mit dem Ziel die Kontrolle über ein Ziel zu erhalten, zu erzeugen. Dies kann auch das Einspeisen eines falschen Zeitsignals in elektrische Steuersysteme umfassen, was zu Fehlfunktionen und Geräteschäden führen kann.

BAUER (2017) erklärt Spoofing ähnlich, als das Aussenden von Signalen, mit der gleichen Struktur wie die Original-GNSS-Signale, auf GNSS-Frequenzen. Die gleiche Struktur bedeutet, dass der Code wie der Original-GNSS-Code ist und die Navigationsnachricht ebenfalls die identische Struktur zur Originalen hat. Der einzige Unterschied findet sich in den Inhalten der Navigationsnachricht. Aufgrund dessen kommt der Empfänger nach der Analyse dieser Inhalt zu einem unterschiedlichen Standort, als seinen Originalkoordinaten. Diese Art der Störsender ist deutlich anspruchsvoller in der Umsetzung als die des Jammings. Neben der erwähnten Art der Navigationsnachrichtenmanipulation, gibt es laut KO (2010) noch die Manipulation des PRN. Diese kann durch Korrelation Fehler im digitalen Signalverarbeitungsprozess verursachen und dadurch PNT-Fehler erzeugen.

Des Weiteren lässt sich Spoofing in gezieltes (targeted) und ungezieltes (untargeted) Spoofing unterteilen (ISLAM et al. 2024). Dabei ist das gezielte Spoofing zeitlich und positionsmäßig synchron und richtet sich auf ein bestimmtes Ziel. Wohingegen das ungezielte Spoofing zeitlich und/oder positionsmäßig asynchron und ohne auf ein festes Ziel abgestimmt ist (ISLAM et al. 2024).

KOVALTSEV et al. (2017) beschreibt den einfachsten Fall des Spoofings. Der Repeater zeichnet Original-GNSS-Signale von einem Empfänger auf und sendet diese mit einem zeitlichen Unterschied weiter. So werden sie von dem Empfänger als Originalsignale verarbeitet. Damit dieser die zeitversetzten Signale wie Originalsignale verarbeiten kann, müssen diese mit einer höheren Energie ausgestrahlt werden als die der Originalsignale, aber weniger als beim Jamming. Da GNSS auf den Pseudostreckenmessungen beruht, führen die zeitverzögerten Signale zu falschen Positionen. Die gezielte Verwendung dieser Repeater wird in der militärischen Nutzung als Meaconing (Abb. 3-6) bezeichnet. MEURER (2024) führt an, dass die Verwendung der Begriffe Repeater, Meaconing und Spoofing nicht eindeutig ist. Es wird in dieser Arbeit, die durch KONOVALTSEV et al (2017) gegebene Definition verwendet.

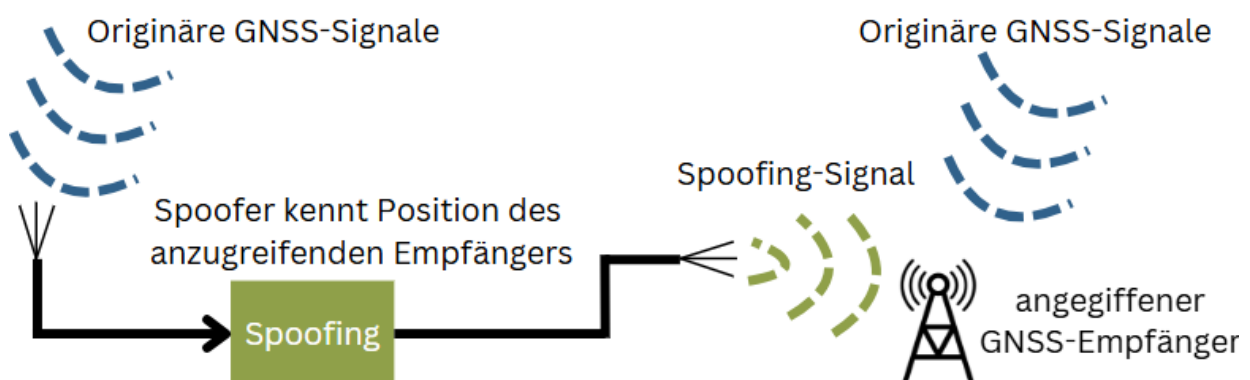


Abb. 3-6: Prinzip des Meaconing (geändert nach BLUM 2022)

MEURER (2024) nennt einige weitere Punkte, die beim Spoofing relevant sind. Zur Nachbildung der GNSS-Signalumbildung am Zielort gibt es zusätzliche Anforderungen für eine „unbemerkte“ Täuschung. Es müssen alle aktuell empfangenen Signale, die aktuelle eigene Position sowie die Position und Geschwindigkeit des Zielobjektes bekannt sein. Es wird eine Signalgenerierung mit der Berücksichtigung von momentaner Codephase und Doppler des Ziels durchgeführt. Außerdem sollten die Vorgaben für Positionen, Geschwindigkeiten oder deren Änderungen realistisch sein, damit das Spoofing nicht auffällt. Da das Täuschsignal von der Position abhängig ist, wirkt es in gewünschter Weise in der Regel nur auf ein Ziel.

Eine Schwierigkeit, die sich dabei zeigt, ist das Täuschen von militärischen Signalen, da der Code unbekannt ist (MEURER 2024). Mithilfe von Spoofing können Fahrzeuge, Flugzeuge und Schiffe unter die eigene Kontrolle gebracht werden, ein Beispiel dazu ist eine Drohne der US-Regierung, dies wird in Unterkapitel 3.3.5 erklärt. Die Wirkung von Spoofing auf Multisensor-Navigationssysteme wie beispielsweise Multi-GNSS-Systeme zum Beispiel GPS und GLONASS ist schwierig vorhersehbar, da der Typ und Algorithmus der Navigationseinheit im Zielobjekt unbekannt sind.

Im Folgenden werden die wichtigsten Unterschiede zwischen Jamming und Spoofing kurz tabellarisch dargestellt (Tabelle 3-1). Diese wurden im Laufe der letzten zwei Unterkapiteln genannt und sind dort detailliert beschrieben. Aufgrund dessen wird im Folgenden auf eine zusätzliche Literaturangabe verzichtet.

Merkmal	Jamming	Spoofing
Definition	Absichtliche Herbeiführung von Interferenzen durch Störsignale auf GNSS-Frequenzen	Erzeugung gefälschter GNSS-Signale mit gleicher Struktur, aber manipulierten Inhalten
Ziel	Erhöhung des Rauschpegels oder Überlastung des Empfängers zur Unterbrechung des GNSS-Empfangs	Irreführung des GNSS-Empfängers zur Ausgabe falscher PNT-Informationen
Signalstruktur	Unspezifisches Störsignal (z.B. Rausch-, CW-, Puls- oder Sweep-Signale), kein GNSS-kompatibles Format	GNSS-kompatibel: gleiche Struktur wie Originalsignal (Code, Navigationsnachricht), aber veränderter Inhalt
Benötigte Störleistung	i.d.R. mehr Leistung als Spoofing	Entsprechend weniger Leistung als Jamming
Technischer Aufwand	Eher gering, insbesondere bei Basic-Jammern	Deutlich höher: Erfordert präzise Kenntnisse von Signalparametern, Codephase etc.
Wirkung auf Empfänger	Unterbrechung von Tracking und Reakquisition, abhängig von J/S-Verhältnis und Distanz,	Fehlpositionierung des Empfängers, durch Manipulation der Navigationsnachricht oder PRN-Information

Tabelle 3-1: Gegenüberstellung von Jamming und Spoofing

Da das GNSS hauptsächlich für die militärische Nutzung erfunden wurde, aber mittlerweile auch viele zivile Nutzer dies verwenden, kann auch der Themenbereich beabsichtigte Störungen durch das Jamming und Spoofing in diese beiden Kategorien gegliedert werden, welche im folgenden Unterkapitel beschrieben werden.

3.3 Ziviles und Militärisches Jamming und Spoofing

Die zunehmende technologische Verwundbarkeit von GNSS macht die Systeme verwundbar für gezielte Störungen wie Jamming und Spoofing. Diese werden sowohl im zivilen als auch im militärischen Kontext gezielt eingesetzt. Das Konzept des Navigation Warfare (NAVWAR) fasst die militärisch-strategische Nutzung von GNSS-Störungen zusammen. In diesem Kapitel werden die unterschiedlichen Akteure, Technologen und Bedrohungsszenarien dargestellt, wobei militärische und zivile Anwendungen ineinander übergehen.

3.3.1 Ziviles Jamming und Spoofing

Im Folgenden werden die zunehmenden Bedrohungen durch zivile GNSS-Störmaßnahmen und deren missbräuchliche Nutzung im Alltag und im städtischen Umfeld betrachtet. Die im Jamming verwendeten Störsender können nach BAUER (2017) und MITCH et al. (2011), welche für diesen Absatz als Literaturnachweis verwendet wurden, in zwei Reichweitenklassen differenziert werden. Der Störsender mit geringer Reichweite sind meist handelsübliche kleine Sender, die Private Protection Device (PPD) genannt werden und in den GNSS-Frequenzbändern Signale senden und damit die Auswertung dieser verhindern. Das verwendete Signal ist das gesweeppte oder Chirp-Signal. PPDs werden, wie der Name schon sagt zum Schutz der eigenen Privatsphäre genutzt, worauf in Unterkapitel 4.3.1 näher eingegangen wird. Es gibt sowohl über den 12V-Zigarettenanzünder im Kfz betriebene PPDs mit einer Reichweite von bis zu 300m, welcher links in Abbildung 3-7 zu sehen ist, als auch batteriebetriebene PPDs (rechts in Abbildung 3-7). Einige können Reichweiten von bis über 10 km erreichen. Des Weiteren werden diese in jene, die ausschließlich das GPS-L1-Signal jammen und solche die sämtliche beziehungsweise mehrere GNSS-Frequenzbänder oder sogar zusätzlich den Mobilfunk stören, kategorisiert. Außerdem handelt es sich um low-cost Jammer, die illegal, aber für jeden zugänglich, im Internet gekauft werden können. Dadurch nehmen Jamming-Vorfälle immer weiter zu. Bei einem britischen Projekt zum Thema wachsende Bedrohungen durch GNSS-Störungen wurden 2014 bis zu zehn Störungen pro Tag erfasst (BAUER 2017). Weitere Anwendungsbeispiele von PPDs sind in den Kapiteln 4.3 zu finden. Diese PPD werden sowohl von zivilen als auch von militärischen Nutzern verwendet.

Störsender mit größerer Reichweite verursachen deutlich mehr Kollateralschäden als solche mit kleiner Reichweite. Als Beispiel für einen Störsender größerer Reichweite nennt BAUER (2017) einen mit 1 mW Sendeleistung sendenden Störer, der ein zehn Meilen entferntes Testschiff gestört hat, sodass dies eine falsche Position und Geschwindigkeit anzeigte, dies führte ohne Alarmmeldung zur Kursänderung durch den Autopiloten. Im weiteren Verlauf wird die von diesen Jammern ausgehende Gefahr weiter beschrieben.

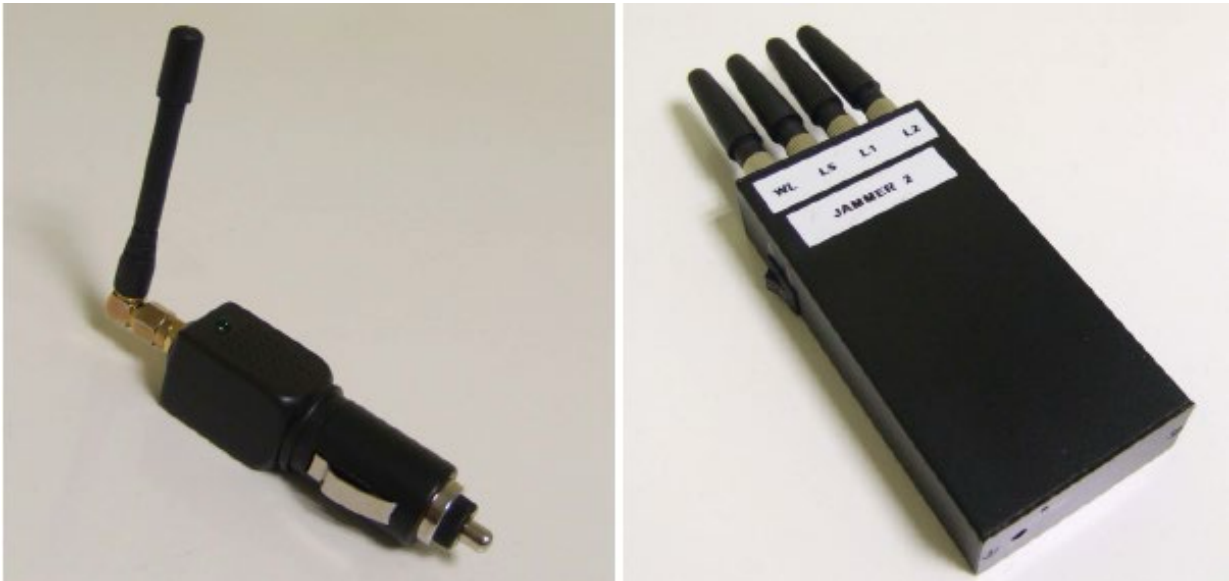


Abb. 3-7: Personal Privacy Device der Bundeswehr (BLUM et al. 2023)

WESTBOOK (2019) zufolge ist für eine fundierte Risiko- und Verwundbarkeitsanalyse der militärischen und staatlichen Führungsebene ein tiefgründiges Verständnis dieser Störmittel zur Grenzbelästigung und Einschüchterung der Menschen nötig. Es sollten hier die Verwundbarkeit und Nähe von Infrastruktur, aber auch in der strategischen Positionierung von eigenen Jamming-Systemen, betrachtet werden. Die geographische Lage eines Staatsgebietes sowie die kritische Infrastruktur sollten bei dieser Risikobewertung einbezogen werden (WESTBROOCK 2019). Aufgrund der allerdings immer populärer werdenden PPDs lässt sich schlussfolgern, dass sich der Themenblock der Reichweiten als nicht mehr ganz so relevant erweist und sollten somit nicht alleiniges Bewertungskriterium sein.

Außerdem lässt sich sagen, dass geographische und geopolitische Aspekte eng mit strategischen Allianzen, Nutzerintentionen, Rüstungsentscheidungen und Besitzverhältnissen von Jamming- und Spoofing-Technologien zusammenhängen. Der Erfolg militärischer Operationen wird maßgeblich vom technologischen Wettbewerb um Jamming- und Anti-Jamming-Systemen abhängig sein. Aufgrund von Aspekten der Kommunikation, Zielgenauigkeit, Aufklärung und Navigation, ist die elektronische Kampfführung ein fester Bestandteil dieser Konflikte.

Ziviles Jamming gewinnt durch die Verbreitung frei verfügbarer Störgeräte zunehmend an sicherheitsrelevanter Bedeutung und wirkt sich in urbanen Räumen zunehmend auf kritische Systeme aus. Dementsprechend werden alternative Navigationsmöglichkeiten (vgl. 5.3) benötigt.

3.3.2 Jamming und Spoofing im militärischen Kontext

Dieses Unterkapitel beleuchtet das gezielte Störung und Täuschen von GNSS-Signalen im militärischen Umfeld. Der Fokus liegt dabei auf taktischen Anwendungen, technischer Umsetzung sowie auf aktuellen Entwicklungen in Konfliktzonen.

Neben der privaten Nutzung von PPDs werden Jammer auch professionell genutzt, dies beschreibt BLUM et al. (2023). Diese professionellen Jammer werden zum Beispiel von Polizei und Militär genutzt. Hierbei handelt es sich sowohl um tragbare Systeme wie drone guns, aber auch großflächige Störungen durch stationäre oder fahrzeugbasierte Systeme. Hier wird das Jamming verwendet, um die Kriegsführung zu beeinflussen und GNSS-unterstützte Waffensysteme abzuwehren und lahm zu legen (BLUM et al. 2023). Professionelle Störsender arbeiten auf mehreren Frequenzen gleichzeitig und sind flexibel programmierbar (FREIMANN 2024). Infolge von zunehmenden Konfliktregionen nehmen Jamming-Vorfälle in dem Ostseeraum (vgl. Baltic Jammer in 4.3.3) und Spoofing-Zwischenfälle im östlichen Mittelmeerraum zu (HEIL 2024). Die Nutzung von Softkill-Systemen wie Jammern, birgt einige Nachteile auf dem modernen Gefechtsfeld. Die Nutzung von Jammern verrät, dass sich dort etwas Schützenswertes befindet und dies führt zu weiteren Handlungen wie elektronische Kampfführung (engl. Electronic Warfare, EW) oder Artilleriebeschuss. Die feindliche kann Artillerie nach erfolgreicher Aufklärung unbeeindruckt von Störmaßnahmen den Jammer zerstören.

Es wird erwähnt, dass sich der enorme Energiebedarf der Störsysteme auf dynamischen Gefechtsfeldern ebenfalls als schwierig darstellt. Neben der bereits erwähnten elektromagnetischen Signatur des Jammers kann es zu starken Einschränkungen der eigenen Kräfte zum Beispiel im Bereich Drohnen, da diese über GNSS gesteuert werden können, kommen.

Bei der Drohnenabwehr werden oft neben GNSS auch die Steuersignale der Drohne gejammt. Hierbei können die erwähnten von einer Person tragbaren Jammer, wie der HP47+ der Bundeswehr (Abb. 3-8) gezielt zur Drohnenabwehr genutzt werden. Dies benötigt allerdings einiges an Vorlauf- und Vorwarnzeit. Bis zum Eintritt der Wirkung dieser drone guns vergehen einige Sekunden im Flug. Dadurch ist die Nutzung meist zu langwierig, um schnellstmöglich die feindliche Drohne zu bekämpfen, da der drone gunner die Drohne erst sieht, nachdem diese bereits im Angriffsflug ist. Sobald allerdings ein Drohnenschwarm auftritt, ist die Drohnenabwehr-Trupp schnell überfordert. Zudem stellt ein tragbarer Jammer dieser Größe immer ein zusätzliches Gewicht, einen extra Ausrüstungsgegenstand und zusätzliche Belastung für den Soldaten dar. Seit Beginn der russischen Invasion geht man aktuell von einer Bekämpfung von 75% der Drohnen mittels Jamming aus.

Drohnen werden nicht nur von tragbaren Jammern, sondern auch durch (große) statische Störsender beeinflusst. Es wird beschrieben, dass nahezu jedes russische Fahrzeug mit einem Jammer ausgestattet ist und in diesem Krieg beide Seiten Störsender verwenden, die Ukraine allerdings etwas weniger. Des Weiteren wird erwähnt, dass tragbare oder statische Jammer, welche den gesamten Bereich stören, deutlich effektiver sind als der Abschuss mit Handwaffen oder drone guns. Im Ukrainekrieg tragen viele Soldaten und Soldatinnen Störsender mit sehr geringer Leistung an ihrer Schutzausrüstung, um sich vor Drohnen zu schützen, dies reicht allerdings nur für private UAV, bei professionell modifizierten Drohnen reicht die Leistung nicht aus. In diesem und dem vorherigen Absatz wurden als Literatur FREIMANN (2024), NAGY (2024) und REISNER (2024) verwendet.



Abb. 3-8: HP47+ (GUSENBURGER 2022)

SÜß (2024) fügt dem Ukrainekrieg hinzu, dass man aufgrund der Informationsdominanz russischer Doktrin vor der Invasion davon ausgegangen ist, dass diese mit der Unterstützung elektromagnetischer Angriffe starten würde. Aufgrund der Verwendung von Störsendern durch Separatisten zu Beginn des Ukrainekrieges 2014 mit der Annexion der Krim wurde mit elektromagnetischen Störungen gerechnet. Dies war nicht der Fall. Es wurden erst im Laufe des Krieges nach der Invasion die elektronischen Maßnahmen eingeschaltet. Da die russischen Truppen ebenfalls GNSS zur Gewinnung von PNT-Informationen nutzen, werden die Störungen der Signale kurz vor Luftangriffen abgeschaltet. Generell lässt sich anhand ihres Berichtes sagen, dass die Bedeutung des Krieges im Weltraum, wo das Thema elektronische Kampfführung, also ebenfalls die beabsichtigte Störung von GNSS, dazuzählt, zunimmt.

Militärisches Jamming ist eng mit der elektronischen Kampfführung verknüpft und stellt durch flexible Einsatzformen eine effektive, jedoch auch risikobehaftete Maßnahme dar. Eine strategische Anwendung von Jamming und Spoofing stellt das im nachfolgenden dargestellte NAVWAR dar.

3.3.3 Navigation Warfare

Navigation Warfare wird laut dem US-amerikanischen DEPARTMENT OF DEFENCE (2021) wie folgt definiert: „Navigation Warfare sind die gezielten defensiven und offensiven Maßnahmen zur Sicherung und Verhinderung von Positions-, Navigations- und Zeitinformationen durch den koordinierten Einsatz von Operationen im Weltraum, im Cyberspace und im Bereich der elektromagnetischen Kriegsführung.“ Dies bedeutet sowohl die Sicherstellung der Verfügbarkeit von PNT durch eigene sowie verbündete Kräfte, aber auch die Unterbindung der gegnerischen Nutzung dieser Informationen. Durch die North Atlantic Treaty Organization (NATO) wird Navigation Warfare sehr ähnlich definiert: NAVWAR bezeichnet die „Verhinderung der feindlichen Nutzung von PNT-Informationen bei gleichzeitigem Schutz der ungehinderten Nutzung der Informationen durch NATO-Streitkräfte und die Wahrung der friedlichen Nutzung dieser Informationen außerhalb des Einsatzgebiets“ (GELSEMA et al. 2012).

In der NATO erfolgt eine differenzierte Betrachtung von NAVWAR in drei Teilbereiche, welche in der Literatur NATO (2008) näher charakterisiert werden. Der defensive NAVWAR umfasst alle Maßnahmen, einschließlich der aus dem Bereich der elektronischen Verteidigung, die darauf abzielen, den Zugang zu sowie die Integrität von PNT-Informationen zu sichern und aufrecht zu erhalten.

Hingegen beinhaltet der offensive NAVWAR sowohl kinetische als auch nicht kinetische Wirkungsansätze, insbesondere elektromagnetische Angriffe, mit dem Ziel, den gegnerischen Zugriff auf PNT-Informationen zu stören oder zu verhindern (NATO 2008). Im Kontext militärischer Operationen richtet sich offensiver NAVWAR insbesondere gegen die gegnerische Systeme zur Führung, Kontrolle, Kommunikation und Datenverarbeitung. Darüber hinaus zielt sie auf waffentechnische Systeme, Fahrzeuge sowie weitere plattformspezifische und PNT-abhängige Systeme ab.

Der NAVWAR-Support beschreibt die unterstützenden Maßnahmen, die primär der Detektion und Analyse von Bedrohungen gegen PNT-Informationen dienen. Um ein umfassendes Lagebild des PNT-bezogenen Operationsraums zu generieren, werden insbesondere Überwachungsmaßnahmen eingesetzt. Somit stellt der NAVWAR-Support eine wesentliche Grundlage für die Planung und Durchführung sowohl offensiver als auch defensiver NAVWAR-Maßnahmen dar (NATO 2008). Die Detektion von beispielsweise Jamming würde dementsprechend unter den Bereich des NAVWAR-Supports fallen und wird im Unterkapitel 5.1 näher behandelt. Das in den Teilbereich offensiver NAVWAR fallende Jamming, wird im gesamten Kapitel 3.2.1 näher erläutert.

NAVWAR ist laut MEURER (2024) ein Teil der Aktivitäten der EW, die zusätzlich in drei Maßnahmen untergliedert wird. Die elektronische Unterstützungsmaßnahmen, welche der

Aufklärung von NAVWAR-Störsignalen dienen, hierzu zählen Detektion, Charakterisierung, Lokalisierung und Unterscheidung der Signale. Im Bereich der elektronischen Gegenmaßnahmen geht es hauptsächlich um die Abstrahlung von Störsignalen mithilfe von elektromagnetischer Energie, gerichteter Energie und beispielsweise in Form von Anti-Strahlungswaffen. Sie sollen die Kampffähigkeit beeinflussen, neutralisieren und zerstören. Die elektronischen Schutzmaßnahmen sollen die Verfügbarkeit, Integrität und Genauigkeit von PNT sicherstellen (MEURER 2024). EW ist ein rein militärischer Kontext, wohingegen NAVWAR sowohl militärische als auch zivile Ziele treffen kann.

Die Zielsetzung von NAVWAR wird in Abbildung 3-9 veranschaulicht. Der grüne Bereich zeigt die Zone, in der ein GNSS-Signal empfangen werden kann. In dieser Zone wurde ein intelligenter Störsender aufgestellt, der in einem gewissen Abstrahlwinkel (blauer Bereich) stört. In diesem lokalen Einsatzgebiet fahren mehrere Panzer, die verbündeten Kräfte (blau) nutzen PPS-Empfänger, feindliche Kräfte nutzen SPS-Empfänger. Nur die SPS-nutzenden Panzer werden gestört. Die innerhalb des Einsatzgebietes liegenden PPS-empfangenden Panzer hingegen haben PNT-Überlegenheit erlangt und können diese taktisch nutzen (MEURER 2024).

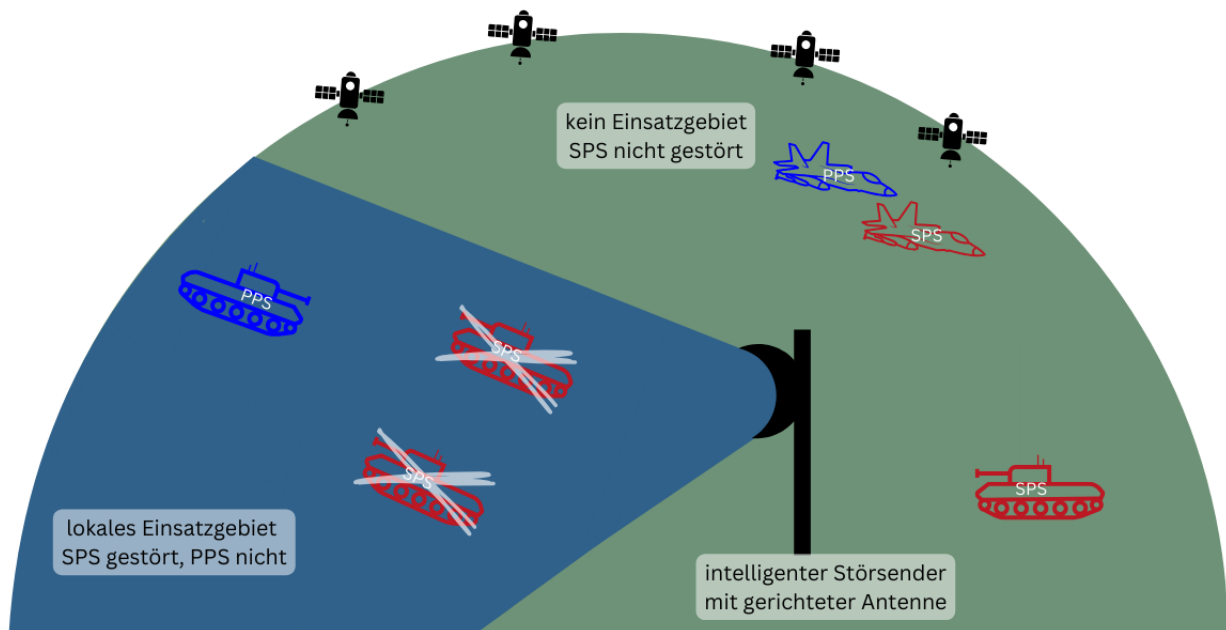


Abb. 3-9: Zielsetzung NAVWAR (geändert nach MEURER 2024)

Die bereits erklärte Differenzierung der Nutzer im Signalaufbau des GPS in autorisierte und nicht autorisierte Nutzer, wurde aufgrund der NAVWAR-Verwendung bereits bei der Errichtung des ersten Satelliten berücksichtigt (MÜLLER 2008). Verbündeten Kräfte erhielten dadurch einen PNT-Vorsprung. Mit der Weiterentwicklung der Signale, insbesondere durch den M-Code, der ein exponiertes Ziel für Störmaßnahmen potenzieller Gegner darstellt (MÜLLER 2008), hat die Relevanz von NAVWAR weiter zugenommen. Der M-Code kann theoretisch gestört werden, dies erfordert jedoch einen hohen technischen Aufwand. Eine effektive Störung setzt Zugang zu starker Sendeleistung, präziser Frequenzkenntnis und die Nähe zum Empfänger voraus.

Dieser Aufwand macht die Umsetzung in der Praxis für nichtstaatliche Akteure schwierig. Zusätzlich zum M-Code wurde der sogenannte spot beam eingeführt. Dieser ermöglicht erhöhte regional begrenzte Signalstärken (MÜLLER 2008), wodurch die Störanfälligkeit in dieser Region reduziert und der Aufwand für gegnerische Kräfte erhöht wird. Durch diese Einführung im Jahr 2018 wurde zusätzlich die gesamte Signalverfügbarkeit erhöht. Insgesamt ist das GPS-Signal eine zentrale Komponente im Bereich der Sicherstellung der Interoperabilität und Einsatzfähigkeit der NATO-Streitkräfte und somit auch im Bereich NAVWAR. Um nicht vollständig abhängig von GPS-Signal und somit von den USA zu sein, wurde der Ausbau des Galileo-Systems weiter gefördert (MÜLLER 2008).



Abb. 3-10: Abschuss von Antisatellitenraketen (THEDARTHDESIGNER 2019)

Zusätzlich zum Stören des Signals gibt es weitere strategische Bedrohungen, die die (militärische) Nutzung von GNSS verhindern. Aufgrund des Umfangs dieser Bachelorarbeit wird an dieser Stelle lediglich ein Überblick gegeben. Ein detaillierter Überblick findet sich in SAALBACH (2025), welcher als Literatur für diesen Absatz und den Folgenden verwendet wird. Dort erfolgt die Einteilung in die Kategorien Antisatellitenraketen, Ko-orbitale Systeme, Cyber-Angriffe und Laserstrahlen zur Blendung oder Zerstörung von Sensoren.

Satelliten, die auf ähnlichen Umlaufbahnen wie die Zielsatelliten unterwegs sind und andere Satelliten stören oder abfangen, werden ko-orbitale Systeme genannt. Der durch Antisatellitenraketen verursachte Weltraumschrott kann genutzt werden, um virtuelle Satelliten zu verstecken. Diese bestehen aus kleinen Teilen in minimal unterschiedlichen Umlaufbahnen und können drahtlos zusammenarbeiten, als wären sie ein Satellit. Der Abschuss solcher Antisatellitenraketen ist in der Abbildung 3-10 zu sehen. Zudem werden immer häufiger Laserwaffen zur Satellitenbeschädigung oder -zerstörung gebaut und teilweise schon vom Militär von bodengestützten, maritimen und luftgestützten Trägerplattformen aus eingesetzt. In allen Bereichen haben die Cyber-Angriffe zugenommen, so auch im Bereich des Satelliten-

Hackings, welche zur Manipulation oder für Spionagezwecke genutzt werden. Da sich dies allerdings als deutlich schwieriger erweist als das klassische Signal-Jamming und -Spoofing, wird es nicht so häufig eingesetzt. Zu den soft skill counterspace capabilities zählen Mittel der elektronischen Kampfführung, sowie das Blenden durch Laser (POHL 2024). Zu den hard skill counterspace capabilities zählen Methoden zur Satellitenzerstörung, wie Antisatellitenwaffen (POHL 2024).

Im Rahmen der NAVWAR stellt insbesondere die gezielte Beeinträchtigung von GNSS-Signalen eine zentrale operative Maßnahme, wie in diesem Unterkapitel beschrieben, dar. Dabei treten verschiedene Formen der Störung auf, die sowohl technologisch als auch strategische Herausforderungen mit sich bringen. Aufgrund der leichten Störbarkeit von GNSS-Signalen werden kombinierte und redundante Navigationsverfahren (vgl. 5.3) benötigt.

3.3.4 Technische Umsetzung und Testszenarien

Zusätzlich zu der Klassifizierung der Störsender in Zivil und Militärisch, können auch Empfänger in diese Kategorien getrennt werden. Die zivilen L1-Band-Empfänger haben bereits ab einem J/S-Verhältnis von 20 dB Signalausfälle, wohingegen der militärisch genutzte Empfänger eine wesentlich höhere Immunität gegen Jamming von teilweise über 40 dB aufweist (FINK 2013). Laut SCHMIDT (2013) kann das maximale J/S-Verhältnis bei militärischen Empfängern bei der Erfassung des zivilen GPS-Signals sogar bis 250 betragen und bei der Erfassung des militärischen Signals bis zu 2500. Die Verfolgung eines einmal erfassten militärischen GPS-Signals erfolgt, auch wenn nach erstmaliger Akquisition das Signal mit bis zu 12.600-mal stärkerem Störsignal gestört wird. Da die auf der Erde empfangene Sendeleistung des GNSS-Signals bei rund $1,6 \times 10^{-16}$ Watt liegt, benötigen Jammer allerdings nur eine Leistung von etwa 2×10^{-16} Watt (SCHMIDT 2013). Daraus lässt sich folgern, dass Störsender eine erhebliche Gefahr für den Verlust der PNT-Informationen darstellen, da sie in der Nähe des Empfängers nur sehr geringe Signalleistungen benötigen, um ihr Ziel zu erreichen. Selbst PPDs können diese Leistungen leicht übertreffen. Militärische Empfänger werden laut SCHMIDT (2013) vor allem Opfer gezielter Jammer und eher weniger derer durch PPDs.

Wie bereits erwähnt gibt es kombinierte GNSS-Störsender, die mehrere GNSS-Signale parallel stören können. Laut FINK (2013) ist zudem eine Kombination aus Jamming und Meaconing möglich. Dabei wird der Empfänger erst gestört und sobald dieser aufgrund fehlender Daten einen regelmäßigen Reset durchführt mittels Meaconing getäuscht. Der Empfänger wird sofern keine externen GNSS-unabhängigen Daten vorliegen, die gefälschten, aber plausiblen Signale als richtig erachten und nutzen (FINK 2013). Daraus lässt sich Schlussfolgern, dass diese Kombination besonders effektiv ist, da sie lange unentdeckt bleiben kann.

Laut KO (2010) gibt es ebenfalls kombinierte GNSS-Empfänger, diese haben neben größeren Bandbreiten auch ein breiteres Spektrum an Trägerfrequenzen als Einzel-Empfänger. Aufgrund dessen müssen gegen diese kombinierten Empfänger Jammer mit höheren Leistungen eingesetzt werden. Da die Entwicklung immer weiter Richtung Multi-GNSS-Empfänger geht, wird weiter an diesen GNSS-Störern geforscht. Außerdem haben die neueren GNSS-Satelliten stärkere Signalleistungen, trotz dessen liegt die minimale Empfangsleistung von GNSS-Empfängern weiterhin im Pikowatt-Bereich. Es schlussfolgert, dass mehrere leistungsschwache und kostengünstige Störgeräte, wie PPDs, eine ernsthafte Bedrohung für zivile Empfänger darstellen kann.

Militärische Empfänger sind zum Beispiel in Marschflugkörpern des Typs Taurus verbaut, welcher in Abbildung 3-11 zu sehen ist. Da in der Erfassungsphase des C/A-Codes nicht erwartet werden kann, dass ein gestörter Empfänger dies trotzdem kann, wurde eine Lösung für den Marschflugkörper gesucht (SCHMIDT 2013). Dieser erfasst den C/A-Code außerhalb des feindlichen Gebietes und schaltet dann auf den mit höherer Störfestigkeit vorhandenen P(Y)-Code um. Die Kryptologie militärischer Empfänger basiert auf dem SAASM-Chip, wobei SAASM für Selective Availability and Anti-



Abb. 3-11: Marschflugkörper Taurus (CARSTENSEN 2024)

Spoofting Module steht (MEURER 2024). Dieses Modul erhöht die Störfestigkeit und verstärkt die Sicherheit für militärische und sicherheitsrelevante Anwendungen.

MITCH et al. (2011) haben sich ebenfalls mit dem Thema kombinierte GNSS-Empfänger und deren Verhalten unter elektronischen Kampfführungseinflüssen beschäftigt. Hier wurden 18 Empfänger auf deren Verhalten getestet, analysiert und die Ergebnisse sind die Vorbereitung für die Entwicklung eines „potenziellen NAVWAR-Prinzips“. Details dazu sind in der genannten Studie zu finden, eine genaue Beschreibung dieses Prinzips wird nicht genannt.

KO (2010) beschreibt außerdem einen vereinfachten Bewertungsablauf von GNSS-Störungen, welches in Abbildung 3-12 zu sehen ist. Hierbei soll der Ablauf zur Verfolgung eines Störsignals beschrieben werden, damit der systematische Mechanismus einer Störung im Empfänger verstanden wird. Das in der Antenne erfasste Signal enthält zusätzlich zum gewünschten GPS-Signal noch das thermische Rauschen des Empfängers sowie unter Störbedingungen auch

Signale von Denial und Deceptive Jammern. Es kommt zu Fehlern in der Verarbeitung der parallelen Code- und Trägerphasenmessungsschleifen, da sich das Denial Störsignal auf das Abtasten und die Quantisierung des Signals auswirkt. Ohne die Einwirkung von Störsignalen liefert die Signalverarbeitung Ausgaben wie Pseudorange, Daten-Demodulation und Dopplerverschiebung, um die Navigation fortzusetzen. Abhängig vom Signal-Rausch-Verhältnis sind dabei Signalakquisition, Trägerverfolgung und Daten-Demodulation. Beim Denial Jamming kann die Signalverfolgung abgebrochen werden, wenn ein J/S-Grenzwert überschritten wird und die Störung ist erfolgreich. Beim Deceptive Jamming wird zur Erzeugung der falschen PNT-Angabe das Störsignal von den Tracking Loops verfolgt, erst dann war das Spoofing erfolgreich.

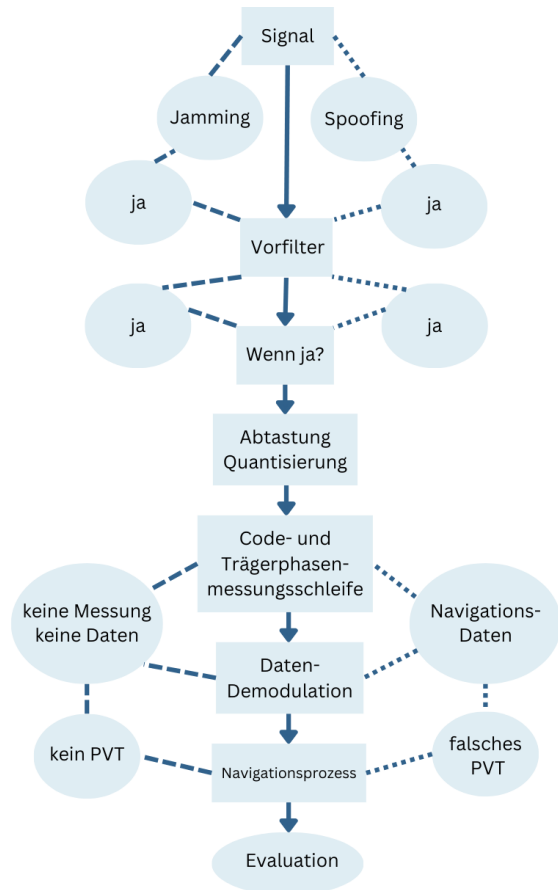


Abb. 3-12: Bewertungsablauf von GNSS-Störungen
(geändert nach KO 2010)

Um das Phänomen des Jammings zu untersuchen, werden laut KASPER (2004) Flugtestungen durchgeführt. Allerdings beschreibt er die zunehmenden Herausforderungen in seiner Studie, die stark gekürzt im Folgenden dargelegt wird. Um mögliche Tests durchzuführen, sollte davon ausgegangen werden können, dass vor der Beschaffung von GPS-gestützten Systemen diese auf ihre Integrität und Zuverlässigkeit getestet wurden. Dies ist leider in einigen Fällen nicht passiert, es wurden anstelle von Testungen unter EW lediglich Experimente durchgeführt, bei denen die Antenne abgehangen wurde oder das GPS manuell ausgestellt wurde. Da in Flugzeugen immer eine Kombination mit INS vorliegt, würde dieser durch Algorithmen aktiviert werden. Da diese Algorithmen nicht nach dem Ein-/Aus-Prinzip funktionieren kommt es zu mehreren Optionen also entweder den normalen standardisierten Betrieb oder die automatische Eliminierung der GPS-Eingaben beim ersten Anzeichen einer GPS-Verschlechterung. Das betroffene Gerät wird das GPS-Signal nicht einfach ignorieren, sondern mittels der Algorithmen seine Eingaben weiterhin qualifiziert mit den anderen verfügbaren Eingaben abwägen.

KASPER (2004) schildert weiterhin, dass eine solche Testumgebung aufgebaut wurde und die wichtigsten Erkenntnisse seien, dass man die militärischen Angehörigen auf den Einsatz von Jammern vorbereiten muss, damit keine Panik entsteht, sobald die PNT nicht mehr über die GPS-Empfänger abgelesen werden kann. Bei den Testungen ist ebenfalls darauf geachtet worden, jede Wahrnehmung der Militärangehörigen zu analysieren, um mögliche Gegenmaßnahmen einleiten zu können. Zudem führte er Test durch, um den Status des GPS-Empfängers zu bewerten. Dazu müssen die einzelnen Empfängerparameter, wie beispielsweise das Träger-Rausch-Verhältnis, der geschätzte Positionsfehler und die Anzahl der verwendeten Satelliten, betrachtet werden. Aus seiner Studie lässt sich folgern, dass solche Testungen weiterhin von großer Relevanz sind, allerdings dies immer schwieriger werden wird, durch den zunehmenden Flugverkehr und die steigende zivile Nutzung von GPS, wodurch der Widerstand aus der Bevölkerung ebenfalls steigen wird. Gerade für die Testung militärischer Jammer wird dies unmöglich werden, da die Besiedelungsdichte zu hoch geworden ist. Trotz dessen ist gerade für die einzelnen Soldaten, aber auch für die obergeordnete Führung ein solches Testverfahren unabdingbar und sollte mit in den Übungsalltag integriert werden.

Aus diesem Grund entwickelte die NATO laut GELSEMA et al. (2012) ein NAVWAR-Testfeld, um in einem realitätsnahen und vernetzten Simulationsumfeld weiter an NAVWAR zu forschen. Ein besonderer Fokus dieses Testfeldes liegt bei der Analyse und Bewertung bewusster Störungen wie Jamming und Spoofing. Es wird beschrieben, dass dieses Simulationsfeld es ermöglicht, verschiedene Szenarien mit aktiven Störquellen möglichst realitätsnah zu simulieren und zu beobachten, wie Plattformen der elektronischen Aufklärung darauf reagieren. Mithilfe des beschriebenen Setups können die Störer geolokalisiert werden, dies kann wiederum von der militärischen Führung genutzt werden für die eigene Kampfführung. Darüber hinaus kann das Testfeld zur Überprüfung und (Weiter-)Entwicklung von NAVWAR-Strategien genutzt werden. Durch die Einspeisung simulierter Störszenarien in reale Analysezellen, lassen sich Verfahren zur Störungsabwehr bewerten und Verbessern. Des Weiteren führen GELSEMA et al. (2012) an, dass durch die Erweiterung durch externe Entwickler, um realistischere Modelle von Jammern, Spoofern und Abwehrsystemen zu integrieren, voranschreitet. So wird es zu einer Plattform für umfassende Untersuchungen und Abwehr bewusster GPS-Störungen in militärischen und sicherheitskritischen Anwendungen.

Auch die Bundeswehr war an Störversuchen in den Jahren 2020 und 2021 beteiligt. Darüber schreiben BLUM et al. (2023), welcher als Literatur die ausführlichen Analyseergebnisse der Masterarbeit BLUM (2022) heranzieht. Aufgrund des Umfangs dieser Ergebnisse und der Länge dieser Bachelorarbeit, wird lediglich ein kurzer Überblick einer Versuchsreihe dazu gegeben. Die Störversuche, waren international organisiert und die Durchführung fand aus sicherheitstechnischen Gründen außerhalb Deutschlands statt. Zudem sind solche Störungen von GNSS-Signalen EU-weit und in den meisten weiteren Ländern verboten. Bei diesen

Versuchen wurden geodätische GNSS-Empfänger des Dezernates V (1) Navigation und Geodäsie des Zentrums für Geoinformationswesen der Bundeswehr (ZGeoBw) verwendet. Eine genannte Versuchsreihe wurde mit einem TG07-Empfänger durchgeführt, welcher 150 m Distanz zu dem jeweiligen Störsender hatte. Die Abbildung 3-13 zeigt die gleichzeitig erfassten Abweichungen für reine GPS-L1 Auswertungen der Pseudostrecken während mehrerer Versuche, die mit EX1 – EX6 gekennzeichnet wurden. Die Abweichungen sind in unterschiedlichen Farben dargestellt, die in der Abbildung erklärt sind. Jeder der sechs Versuche wurde mit einem unterschiedlichen Störsender durchgeführt. Dessen Leistung durch eine dimensionslose Zahl, welche hier als Störleistungsindex in Gelb dargestellt wurde, ausgedrückt wird. In Versuch EX1 sind Abweichungen von bis zu 17 m und ein zunehmender Einfluss der Störleistung auf die Positionsabweichungen detektiert worden. Ergebnisse, die eine besonders konstante Abweichung der Sollkoordinate über den gesamten Jammingzeitraum aufweisen, sind besonders gefährlich (BLUM et al. 2023). Daraus lässt sich schlussfolgern, dass der in Versuch EX1 verwendete Störer gerade für die Nutzung längerer Zeiträume sinnvoll ist, da er die Position mit einer nahezu konstanten Abweichung beeinflusst. Aus den Versuchen EX4 bis EX6 kommen BLUM et al. (2023) zu dem Ergebnis, dass es bei steigender Störleistung dieser drei GNSS-Störsendern zu kompletten Auswerteverlusten kommt.

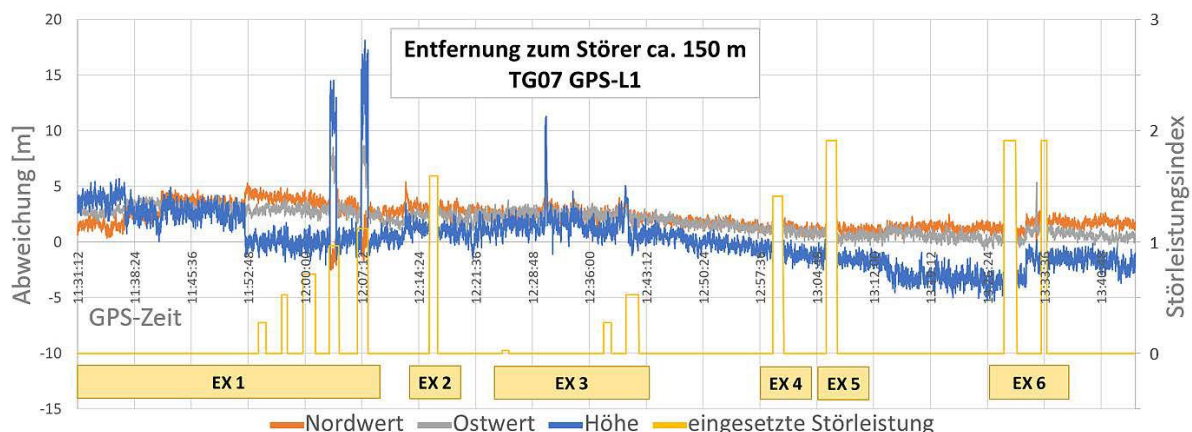


Abb. 3-13: Störung der GPS-L1-Frequenz auf 150m Entfernung zum Störsender (BLUM et al. 2023)

Die beschriebenen Tests und Technologien zeigen die Notwendigkeit robuster Gegenmaßnahmen, sowohl durch technische Innovationen als auch durch realitätsnahe Übungsszenarien. Außerdem wird verdeutlicht, wie relevant die weitere Forschung zum Thema Störung von GNSS ist.

3.3.5 Geopolitische und sicherheitsrelevante Entwicklungen

Die Organisation C4ADS analysiert in ihrem Bericht aus dem Jahr 2019 GPS-Spoofing in Russland und Syrien, eine Zusammenfassung wird im Folgenden gegeben. Insgesamt wurden von Februar 2016 bis zur Berichtserstellung knapp 10.000 mutmaßliche Fälle an zehn Standorten auf 1.311 Schiffnavigationssysteme detektiert. Des Weiteren konnten Zusammenhänge zwischen dem Schutz von VIPs, wie Staatsoberhaupt Wladimir W. Putin, und russischen GNSS-Spoofings festgestellt werden. Diese betrafen ebenfalls die zivile Infrastruktur des Landes. Hier liegt außerdem der Verdacht nahe, dass es sich um mobile Systeme handelt. Spoofingaktivitäten an geschützten Einrichtungen wurden auch an der russischen Küste oder auf der Krim detektiert. In aktiven russischen Kampfgebieten wie Syrien wurde die Fähigkeit ebenfalls genutzt, um den Luftraum zu sperren. Laut C4ADS wird dabei allerdings die Öffentlichkeit nahezu nicht beeinträchtigt.

In seinem Artikel erwähnt WESTBROOK (2019) einige Vorfälle von militärischem Jamming und Spoofing. Dieser gilt, wenn nicht anders gekennzeichnet als Literatur für die nachfolgend in diesem Unterkapitel genannten Beispiele. Des Weiteren wird in den folgenden zwei Absätzen von Jamming gesprochen, hier ist das Spoofing mit inkludiert.

Auch bereits vor der russischen Invasion auf die Ukraine wurden bei Überwachungstätigkeiten in der Ukraine schwere GPS-Störungen detektiert. Neben der Desorientierung von Präzisionswaffen wurden auch dort bereits Langstreckendrohnen bei der Aufklärungs- und Zielerfassung gestört. Zusätzlich zum GPS vielen die Steuer- und Kommunikationssysteme inklusive der Backup-Systeme aus. Neben mehreren von ihm genannten Jamming-Vorfällen nennt er ebenfalls Beispiele, an denen die Position von Drohnen oder Präzisionswaffen gespoofed wurden. Ein mediaausgenutztes Beispiel stellt die durch iranisches Spoofing hervorgerufene Landung einer US-amerikanischen militärischen Drohne auf iranischem Gebiet dar. Nach diesem Landungszwang der iranischen Regierung warfen diese den USA Spionage vor und versuchten Berichten zufolge die Drohne nachzubauen (WESTBROOK 2019). Es ist stark umstritten, ob es sich hier tatsächlich um GNSS-Spoofing gehandelt hat. Die kritische Betrachtung kann in diverser Literatur wie WESTBROOK (2019) oder RAWNSLEY (2011) nachvollzogen werden. Insgesamt sind wirkliche Fälle von targeted Spoofing außerhalb von Test-Umgebungen nicht gesichert bekannt. Entsprechend der Klassifikation des Spoofings von ISLAM et al. (2024), handelt es sich hier um targeted Spoofing, da die Störung sich direkt gegen ein Ziel richtet. Ein Beispiel welches als untargeted Jamming bezeichnet werden könnte, ist das russische Pole-21-system. Dies sieht laut WESTBROOK (2019) vor, landesweit Störsender auf kritischen Infrastrukturen zu platzieren, um sich auf konventionelle Kriege vorzubereiten. Auch in Bürgerkriegsszenarien wird Jamming und Spoofing eingesetzt.

China soll insbesondere im territorialen Kontext GPS-Störungen gegen US-Streitkräfte und seine Nachbarn hervorgerufen haben. Nordkorea nimmt beispielweise zivile Auswirkungen, um mit Absicht wirtschaftlichen Schaden und Schikane zu bewirken, bei Störungen militärischer und ziviler Luft- und Seeverkehrssysteme in Kauf. Auch



Abb. 3-14: russisches Störsendersystem (SAPWOOD 2024)

Nordkorea ist bekannt für seine grenzübergreifenden Großraumstörungen. Diese reichen bis zur Metropolregion des südkoreanischen Seouls und betreffen somit zivile und militärische Empfänger. Ähnliche Vorfälle gibt es auch im europäischen Raum, hauptsächlich an den zu Russland grenzenden Staaten. 2019 hat Norwegen Russland für 27 Störungen von GNSS-Signalen verantwortlich gemacht, die meisten davon während einer großangelegten NATO-Übung (KERN 2024). Das russische Störsystem R-300Zh Zhitel ist in Abbildung 3-14 zu sehen.

Im Falle eines militärischen Konflikts zwischen zwei oder mehr Akteuren, sei es staatlich oder nicht, könnte die kombinierte Verwendung militärischer Störsender und zahlreicher ziviler Kleinstgeräte, wie PPDs, zu massiven Störungen führen (WESTBROOK 2019). Darüber hinaus besteht die Befürchtung, dass gezielte Störungen mit weiteren elektronischen und cyberbasierten Angriffen kombiniert werden. Nicht nur in Übungen oder im Kriegsfall werden Jammer und Spoofer eingesetzt.

Da der Handel, die Herstellung und Nutzung von PPDs immer weiter zu nehmen, wächst die Gefahr des zivilen Jammings immer weiter. Gerade in dichtbesiedelten urbanen Räumen ist es unrealistisch Sicherheitsabstände zwischen kritischer Infrastruktur zu schaffen. Insgesamt lässt sich also anhand der Aussagen von WESTBROOK (2019) zusammenfassen und schlussfolgern, dass Jamming mittlerweile keine rein militärische Bedrohung mehr darstellt. Sondern gerade auch durch die Nutzung der Privatsphäre schützenden kleinen Jammer, welche missbräuchlich verwendet werden, werden die zivilen, sicherheitsrelevanten Auswirkungen und Risiken immer weiter voranschreiten.

Die geopolitischen Entwicklungen und gezielten GNSS-Störungen zeigen, dass Jamming und Spoofing längst ein globales Machtinstrument mit hohen Eskalationspotenzial sind. Insgesamt wird das zivile und militärische Jamming und Spoofing immer relevanter, aber auch die Grenzen zwischen den beiden Nutzergruppen verschwimmt immer weiter. Die Auswirkungen dieser steigenden Nutzung auf verschiedene Bereiche werden im folgenden Kapitel näher beleuchtet.

4 Auswirkung von Jamming und Spoofing

Nachdem bereits in Unterkapitel 2.2 die Anwendungsfelder von GNSS beschrieben wurden, werden sie in diesem Kapitel auf deren Auswirkungen analysiert und bewertet. Im Fokus steht dabei, wie sich die gezielten Eingriffe durch beabsichtigte Störungen wie Jamming und Spoofing auf reale Anwendungen auswirken, sowohl allgemein als auch in ausgewählten sicherheitsrelevanten Bereichen. Insbesondere die Schifffahrt, der Straßenverkehr und der Luftraum sind stark von GNSS-Diensten geprägt und damit besonders anfällig für Interferenzen. Ziel dieses Kapitels ist es, die potenziellen Gefahren durch Jamming und Spoofing praxisnah zu erfassen. Die Auswirkungen wurden durch die Autorin unabhängig von Literatur bewertet, es sei denn es ist anders gekennzeichnet.

4.1 Allgemein

Bei der Nutzung von Störsendern, sei es Jammern oder Spoofern, werden sowohl beabsichtigte als auch unbeabsichtigte Gefahren und Auswirkungen hervorgerufen. Eine unbeabsichtigte Gefahr stellte, WESTBROOK (2019) zufolge, ein Lieferfahrer da, der sich der Kontrolle seines Arbeitgebers entziehen wollte. Dieser nutzte seinen PPD und verfälschte damit unabsichtlich 2013 den Zeitstempel der Londoner Börse mit (WESTBROOK 2019). Die Auswirkungen bei der auf hochpräzise Zeitsynchronisation angewiesenen Börse, waren erheblich und führten zu negativen Entwicklungen des Kurses. Diese unbeabsichtigte Auswirkung zeigt, wie selbst kleine Manipulationen durch Jamming gravierende wirtschaftliche Schäden verursachen können und verdeutlichen die Notwendigkeit robuster Schutzmechanismen für zeitkritische Infrastrukturen. Des Weiteren lässt sich schlussfolgern, dass auch kleine PPDs immense unabsichtliche Auswirkungen haben können.

Je nach ausgebildeter „Intelligenz des Empfangssystems“ können Störungen weitreichende Folgen bis hin zum Totalausfall beinhalten (FINK 2013). Dies unterstreicht, dass die Empfängerseite eine entscheidende Rolle bei der Abwehr von Störungen spielt, weshalb technische und algorithmische Verbesserungen dringend notwendig sind. Durch Störsender oder ausgefeilte Spoofing-Methoden können GNSS-Hacker die extremen Zeitsensibilitäten bei Finanztransaktionen aus der Ferne ausnutzen, um Geld effektiv aus den Netzwerken der Händler verschwinden zu lassen (RETERSKI 2015). Gerade bei zeitkritischen Netzwerken, kann ein fehlerhafter Zeitabgleich erhebliche Auswirkungen haben.

Ein Ausfall im Bereich des Zugverkehrs, welches sowohl GNSS als auch die Zeitinformation von GNSS nutzt, könnte zu Unfällen und einer Art Dominoeffekt führen (FINK 2013). Die potenzielle Gefährdung der öffentlichen Sicherheit durch Jamming und Spoofing im Transportwesen verdeutlichen den Handlungsbedarf, insbesondere bei sicherheitskritischen Systemen. Diese Gefahren sollten unbedingt vermieden werden, mögliche Maßnahmen zur Detektion und

Gegenmaßnahmen von Jamming und Spoofing sind im Kapitel 5 zu finden. RETERSKI (2015) nennt ein Beispiel, bei dem die System-Anfälligkeit der präzisen Zeitmessung bereits vor der Störung des GPS bemerkt wurde. Hierbei handelt es sich um die Umspannwerksuhren des Modells 1094B, diese weisen eine Schwachstelle gegenüber professionellen Jamming auf. Als Reaktion darauf, wurde ein gegen GPS-Störungen geschütztes Modell entwickelt.

4.2 Im zivilen und militärischen Kontext

Aus den in Unterkapitel 3.3 dargestellten Beispielen zum Thema ziviles und militärisches Jamming und Spoofing lassen sich zusätzlich Auswirkungen herausstellen. Neben der offensichtlichen Auswirkung, dass die PNT-Informationen fehlerhaft sind und somit die operative Kampfführung beeinträchtigt ist, kann es zusätzlich Gefahrenpotentiale für Hinterhalte oder Fallen darstellen. Ebenfalls kann abgeleitet werden, dass diese Störmethoden sich auch auf die Moral der Truppe auswirken, da diese nicht im gewohnten und den Umständen entsprechend sicheren Rahmen operieren kann.

Dies wird durch die bereits in Unterkapitel 3.3.1 erwähnte zivile Auswirkung der Schikane und Einschüchterung als offensives und politisches Mittel gestärkt (WESTBROOK 2019). Trotz dessen hat es bisher keine schwerwiegenden Folgen über symbolische politische Signale hinaus durch die gezielte Störung ziviler Infrastruktur gegeben (WESTBROOK 2019). Die psychologische Wirkung dieser Störungen als Mittel der Einschüchterung ist erheblich, auch wenn materielle Schäden bisher meist begrenzt blieben. Es kann jedoch die Eskalationsdynamik begünstigen. Deutlich gravierendere Folgen lassen sich bei Jammingmaßnahmen über mehrere Tage ableiten. Dies könnte zusätzlich zum Frust der Bevölkerung, dem politischen Druck zu Aufständen, schweren Unfällen oder Eskalation führen. Langfristige Störmaßnahmen können somit die gesellschaftliche Stabilität gefährden und stellen ein erhebliches Risiko für öffentliche Sicherheit und Ordnung dar.

Bei der Nutzung von Spoofing zum Verleiten zu unbefugten Grenzübertritten, wie durch die US-amerikanische Drohne (vgl. 3.3.5), kann eine Auswirkung die Verstärkung der territorialen Spannungen zwischen den betroffenen Ländern sein. Dies geschah RETERSKI (2015) zufolge ebenfalls während des „Google-Maps-Krieges“, bei dem ein nicaraguanischer Militärkommandeur auf Grund einer fehlerhaften Darstellung eines Abschnittes eines abgelegenen Teils der Landesgrenze zu Costa Rica den Befehl zum Grenzübertritt rechtfertigte. Solche Vorfälle illustrieren, wie GNSS-Spoofing zu politischen Krisen und internationalen Konflikten beitragen kann, was die Bedeutung von Schutzmaßnahmen auf staatlicher Ebene unterstreicht. Des Weiteren sagt RETERSKI (2015), dass mittels GNSS-Störer in militärischen Kontexten nicht zwingend die Kontrolle über die gegnerischen Materialien erlagt, sondern das Schlachtfeld vernebelt werden soll. Außerdem sind EW-Plattformen immer die ersten

Konfliktziele. Die taktische Nutzung von Jamming und Spoofing beeinflusst direkt die Kriegsführung und erfordert neue militärische Strategien und Schutztechnologien.

KASPER (2004) differenziert ebenfalls in militärische und zivile Schwachstellen. Zusätzlich zu den im vorherigen Abschnitt herausgestellten Auswirkungen kann es durch GNSS-Störungen zu höheren Waffenausgaben, einem Anstieg des Kollateralschadens, sowie zu friendly fire⁶ kommen. Aber auch Verzögerungen bei der Zielfindung und erhöhte Bedrohungsanfälligkeit sind möglich. Insgesamt kann man daraus folgern, dass es wenig Zweifel darangibt, dass GNSS-Störungen die Verwirklichung operativer Konzepte nicht beeinflussen und zu anderen Ergebnissen in Entscheidungsprozessen führen. Diese Effekte erhöhen das Risiko und die Kosten für militärische Operationen erheblich und machen robuste Gegenmaßnahmen (vgl. 5.2) unverzichtbar. Als zivile Schwachstelle führt er all diejenigen Einrichtungen an, die eine Abhängigkeit von GNSS für Navigation und/oder Zeitmessung haben. Besonders hebt er Bereiche der kritischen Infrastruktur, sowie die in den nachfolgenden Unterkapiteln beleuchteten Bereichen, hervor. Die starke zivile Abhängigkeit von GNSS-Systemen macht den Ausfall oder eine Manipulation zum Risiko für die Gesellschaft und Wirtschaft insgesamt.

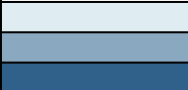
RETERSKI (2015) hat in seinem Artikel die angeführte Matrix (Tabelle. 4-1) zu den Auswirkungen und Bedrohungen von GNSS-Jamming durch verschiedene Akteure in Bezug auf ausgewählte zivile und militärische Anwendungsbereiche visualisiert. Sie differenziert in fünf Akteursgruppen, vom (unbeabsichtigten) Störenden bis hin zu staatlichen Streitkräften. Diese Akteure werden hinsichtlich ihres potenziellen Einflusses auf verschiedene Bereiche analysiert, diese werden in vier Hauptgruppen unterteilt. Die Hauptkategorien heißen nationale Infrastruktur, staatliche Operationen, Operationen im Privatsektor sowie Militär- und Sicherheitssektor. Die farbliche Kodierung differenziert zwischen den Einflüssen der Bedrohungen.

Der Matrix lässt sich entnehmen, dass insbesondere kritische Infrastrukturen, wie Eisenbahn, Straßen- und Schiffsverkehr sowie das Stromnetzmanagement in besonderem Maße durch Aufständische/Terroristen und staatliche Streitkräfte bedroht sind. Im Bereich des Privatsektors zeigen sich vor allem Lieferketten, Finanztransaktionen und automatisierte Landmaschinen anfällig gegenüber organisierten Kriminellen und gezielten Angriffen staatlicher Akteure. Der Militär- und Sicherheitssektor weist insgesamt das breiteste Bedrohungssektum auf, wobei insbesondere UAVs, militärische Kommunikation und VIP-Schutzdienste eine hohe Bedrohungslage durch nahezu alle Akteursgruppen aufzeigen. Dieser Matrix kann man entnehmen, dass der Einfluss in den meisten Bereichen entweder hoch oder niedrig ist, eher selten allerdings mittelmäßig. Man kann außerdem aufgrund der Nutzergruppen erkennen, aus

⁶ unabsichtlichen Beschuss eigener oder verbündeter Kräfte (KASPER 2004)

welcher Motivation die Störsender eingesetzt wurden in Zusammenhang mit deren Bedrohungsstärke. Die Tabelle 4-1 bietet damit eine strukturierte Übersicht über potenzielle Stör- und Angriffsvektoren auf GNSS-abhängige Anwendungen, insbesondere im Kontext von Sicherheits- und Verteidigungsstrategien. Die differenzielle Betrachtung der Akteursgruppen und Zielbereiche macht deutlich, dass Sicherheitsstrategien maßgeschneidert sein müssen, um vielfältigen Bedrohungen wirksam zu begegnen.

	(unbeabsichtigte) Störende	(opportunistische) Kriminelle	(organisierte) Kriminelle	Aufständische/ Terroristen	staatliche Streitkräfte
nationale Infrastruktur					
Eisenbahn					
Flussicherung					
Straßenverkehr					
Seeverkehr					
Hafenaktivitäten					
Stromnetzmanagement					
staatliche Operationen					
Fischereimanagement					
Notfall- und Katastrophenhilfe					
Operationen im Privatsektor					
Finanztransaktionen					
Lieferketten					
Bauwesen					
Bergbau					
Öl- und Gasbohrungen					
automatisierte Landmaschinen					
Militär- und Sicherheitssektor					
UAVs					
autonome Unterwasserfahrzeuge					
Militärische Kommunikation					
VIP-Schutzdienste					



niedrige Auswirkung/Bedrohung

mittlere Auswirkung/Bedrohung

hohe Auswirkung/Bedrohung

Tabelle 4-1: Bedrohungsmatrix von GNSS-Jamming (geändert nach RETERSKI 2015)

Aus RETERSKI (2015) lässt sich folgern, dass ein sehr großes Gefahrenpotential von den Nutzern selbst ausgeht. Die Abhängigkeit des Menschen von GNSS und mobilen Geräten kann die Fähigkeiten der Benutzer beeinträchtigen. Im Falle von GNSS-Störungen wissen die Menschen nicht mehr, wo sie sind, wo Notausgänge oder Gefahrenbereiche sich befinden. Dies zeigt die Notwendigkeit, Nutzer besser zu schulen und alternative Navigationsverfahren (vgl. 5.3) zu entwickeln, um Resilienz gegenüber GNSS-Ausfällen zu erhöhen.

4.3 In ausgewählten Bereichen

Nachdem im vorherigen Kapitel die allgemeinen, zivilen und militärischen Auswirkungen von GNSS Jamming und Spoofing erläutert wurden, soll nun eine detaillierte Betrachtung der Auswirkungen in besonders GNSS-abhängigen Bereichen erfolgen. Die folgenden Unterkapitel analysieren exemplarisch die maritimen, luft- und bodengestützten Anwendungen. Diese Bereiche wurden bereits in Unterkapitel 2.2 genauer beschrieben. Diese Sektoren gelten aufgrund ihrer hohen Automatisierung und Navigationsabhängigkeit als besonders anfällig gegenüber GNSS-Störungen. Ziel ist es, praxisnahe Auswirkungen sowie potenzielle Sicherheitsrisiken aufzuzeigen, die durch gezielte oder unbeabsichtigte Störungen entstehen können. Dabei werden sowohl konkrete Vorfälle als auch systematische Schwachstellen beleuchtet, um ein umfassendes Bild der Bedrohungslage zu vermitteln.

4.3.1 Auf bodengebundene Anwendungen

Die Abhängigkeit von GNSS im Straßenverkehr, welche in Unterkapitel 2.2.1 beschrieben wurde, lässt auch darauf schließen, dass die Nutzung von Jamming und Spoofing immer weiter zunimmt. Störungen durch Jamming und Spoofing bergen erhebliche Risiken für die Verkehrssicherheit und Funktionssicherheit.

Ein großes Bedrohungspotential bergen die PPDs. BAUER (2017) zufolge kann in zwei Anwendungsarten unterschieden werden. Bei der Verwendung der PPDs zum Eigenschutz möchte der Kfz-Fahrer seinen Standort schützen, um sich beispielsweise den Kontrollen des Chefs zu entziehen (BAUER 2017). Eine Auswirkung dabei ist selbsterklärend, wenn man beachtet, dass ein solcher PPD nicht gezielt nur den GNSS-Empfänger des eigenen Fahrzeuges. Sondern auch die der umliegenden Fahrzeuge gestört werden. Das diese PPDs allerdings nicht auf Empfänger, die in Fahrzeugen verbaut sind, konditioniert werden können kommt es hier immer wieder zu Zwischenfällen. Das in Unterkapitel 4.1 erwähnte Stören der Börse wurde durch einen solchen Lieferfahrer mittels PPD verursacht, da dieser seine Route vor dem Management verbergen wollte (SAALBACH 2025). Auch für Arbeitszeitbetrug werden PPDs beispielsweise von Londoner Liefer- und Taxifahrern verwendet (RETERSKI 2015). BAUER (2017) nennt ein bekanntes Beispiel, ein Müllwagen-Fahrer, der Ende 2009 von einer Autobahn aus das GBAS des Flughafens Newark unbewusst täglich störte. Dies führte zu Ausfällen und verzögerte den Flugbetrieb. Der Grund für die Nutzung des PPDs wurde nicht veröffentlicht. Die Nutzung von PPDs mit scheinbar harmloser Motivation führt in der Praxis zu erheblichen Störungen ganzer Verkehrssysteme und zeigt, dass bereits individuelle Eingriffe unkontrollierbare Kollateralschäden verursachen können.

Die zweite Anwendungsart ist BAUER (2017) zufolge die böswillige Absicht hinter der Nutzung von PPDs. Ein genanntes Beispiel ist eine GNSS-abhängige Erhebung von Gebühren zu sabotieren. Gemeint sind hier beispielsweise Mautgebühren für LKW, da die Gebühren bei GNSS-Störungen nicht automatisch abgebucht werden können. Daraus lässt sich die Auswirkung des Betruges von Gebühren schlussfolgern. In der Abbildung 4-1 wird ein solcher Jamming-Fall dargestellt. Hierbei werden die umliegenden Fahrzeuge ebenfalls gestört (blauer Kreis). Der LKW, welcher einen PPD mitführt, ist rot dargestellt. Solche

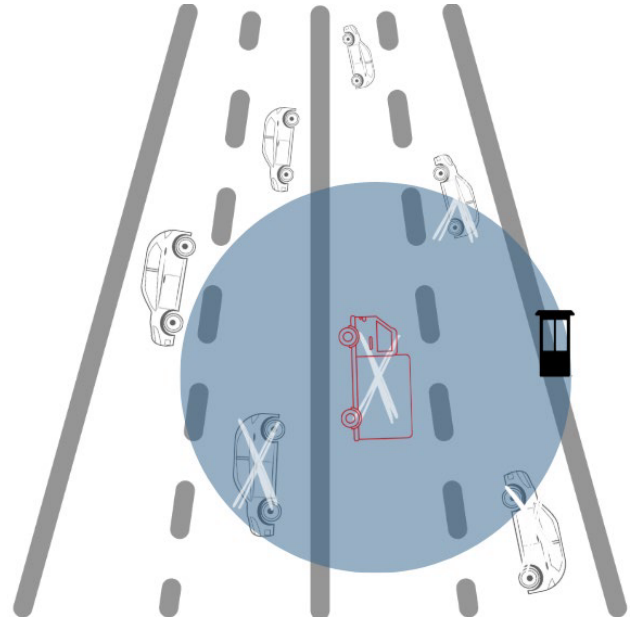


Abb. 4-1: Auswirkungen von Maut-Jamming (erstellt nach BAUER 2017)

betrügerischen Handlungen gefährden nicht nur den ordnungsgemäßen Betrieb automatisierter Kontrollsysteme, sondern stellen eine gezielte Schwächung öffentlicher Infrastruktur dar.

Die Auswirkung des Betruges lässt sich ebenfalls aus dem durch BAUER (2017) beschriebenen Vorfalls des Versicherungsbetruges ziehen. Es gibt Versicherungen die ihren Tarif über die durch GNSS bestimmten Parameter, wie Geschwindigkeiten und den Standort ermitteln. Die Manipulation dieser Daten untergräbt datenbasierte Geschäftsmodelle und führt zu systematischen Schäden. Dies legt eine Verleitung zur böswilligen Nutzung von PPDs nahe, um Geld zu sparen und einen eigenen Vorteil zu erschleichen. Da nicht empfängerspezifisch gestört wird, sondern allgemein, kann es als Auswirkung wieder zu größeren Schäden kommen.

Beim Diebstahl von Baumaschinen, welcher zur Überwachung mit einem GNSS-Empfänger ausgestattet sind, kommen ebenfalls PPDs zum Einsatz (BAUER 2017). Die durch GNSS-gestützte Sicherheitssysteme erzielte Abschreckung wird durch den Einsatz einfacher Störgeräte mit gravierenden wirtschaftliche Folgen wirkungslos. Der Missbrauch von GNSS-Störungen zum persönlichen Vorteil gefährdet Dritte erheblich, da er systematische Lücken im GNSS ausnutzt und ganze Sicherheitsmechanismen beeinträchtigt. Die Auswirkungen sind identisch, da hier der eigene Vorteil über das Allgemeinwohl und andere GNSS-Nutzer gestellt wird. All diese Sozio-technischen Veränderungen, wie Trackingsysteme, automatische Mauterfassung, aber auch GPS-basierte Spiele wie Pokémon-Go (WESTBROOK 2019), führen zu einer vermehrten Nutzung von kleinen Störsendern und die Motivation für den Erwerb wächst. Die Verbreitung solcher Technologien im Alltag erhöht die Anzahl potenzieller Störquellen exponentiell und senkt zugleich die Hemmschwelle für deren Nutzung mit weitreichenden sicherheitsrelevanten Folgen.

Ein in Braunschweig durchgeführter Feldversuch in der Nähe einer deutschen Autobahn und dem Flughafen Braunschweig-Wolfsburg belegte systematisch das reale Ausmaß von GNSS-Störungen im Straßenverkehr (STANISAK et al. 2016). Innerhalb von zwei Wochen wurden mehrere hundert Interferenzereignisse festgestellt, davon etwa 14% mit hoher Priorität in der dargestellten Intensitätsskala und deutlich messbaren Auswirkungen auf präzise GNSS-Empfänger. Die hohe Anzahl realer Störungen unterstreicht die Dringlichkeit für Überwachungs- und Schutzmaßnahmen, um die Sicherheit vernetzter Verkehrsanwendungen zu gewährleisten. Viele dieser Störungen lassen sich STANISAK et al. (2016) zufolge auf PPDs zurückführen. Sobald eine Störung auftritt, ist dies sowohl in der Anzahl der erkannten Satelliten zu sehen als auch im Carrier to Noise Ratio (Abb. 4-2). In diesem konkreten Fall ist zusehen, dass zwei Satelliten ihre Verbindung zum Empfänger vollständig verlieren. Die übrigen sieben Satelliten verlieren lediglich ihre Positionsgenauigkeit. Durch die Carrier to Noise Ratio lässt sich das Störereignis detektieren, darauf wird allerdings in Unterkapitel 5.1 näher eingegangen. Die Ergebnisse aller Versuche deuten darauf hin, dass PPDs eine wachsende und ernstzunehmende Bedrohung in der Verfügbarkeit, Integrität und Funktionssicherheit satellitengestützter Navigationssysteme darstellen. Um dieser Entwicklung zu begegnen sind langfristige, standortübergreifende Studien sowie technische Schutzmaßnahmen zwingend erforderlich, um die Auswirkungen auf umliegende Systeme einschließlich kritischer Infrastruktur zu minimieren.

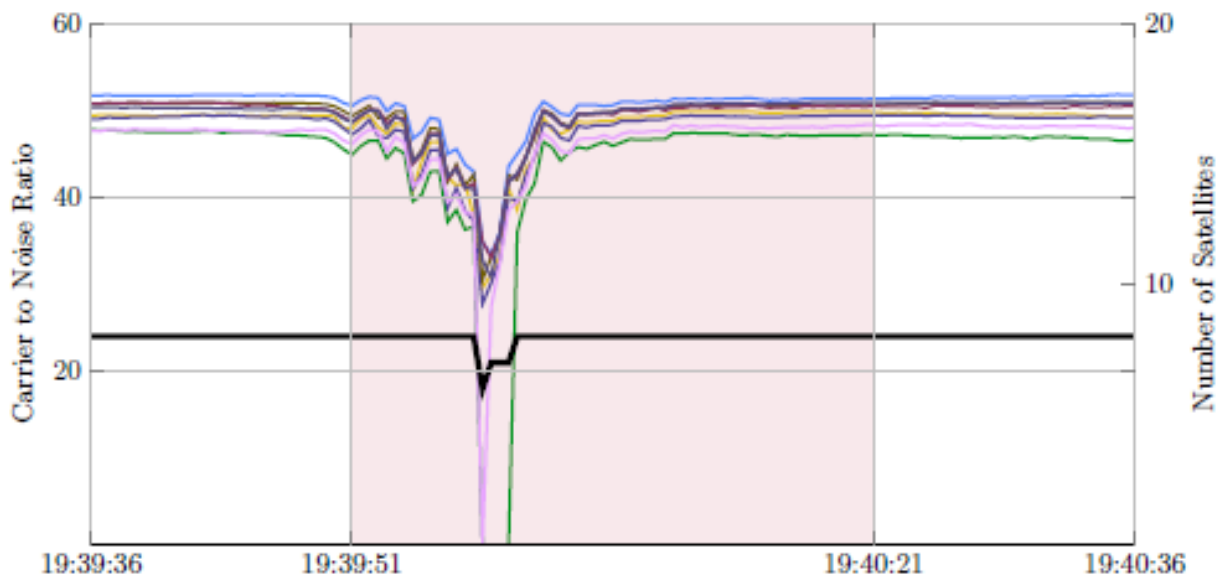


Abb. 4-2: Störauswirkungen auf Satellitenanzahl und Carrier to Noise Ratio (STANISAK et al. 2016)

Der Bericht „Global Positioning System (GPS) Interference“ der US-Behörde CISA (Certified Information Systems Auditor) beschreibt einen GPS-Jamming-Vorfall im Januar 2022 am Flughafen Denver (CISA 2022). Bei diesem Vorfall waren über 33 Stunden zahlreiche Infrastrukturbereiche durch starke Interferenzen beeinträchtigt. Die lange Dauer des Vorfalls und die Vielzahl betroffener Systeme belegen die hohe Verwundbarkeit selbst großer,

sicherheitsrelevanter Einrichtungen gegenüber GNSS-Störungen. Trotz eines etablierten Koordinationsprozesses gelang die Lokalisierung und Behebung der Störung nur verzögert (CISA 2022). Gründe hierfür lagen GOWARD (2023) zufolge vermutlich in unklaren Zuständigkeiten, fehlender technischer Infrastruktur sowie begrenzten Ressourcen der zuständigen Behörden. Die strukturelle Unterschätzung von GNSS-Störungen im Behördenapparat stellt eine große Gefahr dar. Die organisatorische Resilienz ist hier genauso wichtig wie die technische. Die Auswirkungen reichten vom Ausfall luftfahrtbezogener GPS-Dienste über Störungen in Telekommunikationsnetzen bis hin zu Problemen im öffentlichen Sicherheitsfunk. Eine öffentliche Warnung erfolgte nicht, was zu unnötigen Fehlersuchen und potenziellen Sicherheitsrisiken führte (GOWARD 2023). Die Ergebnisse der Analyse des Vorfalls von GOWARD (2023) verdeutlichen, dass GPS-Störungen erhebliche praktische und sicherheitsrelevante Folgen haben können. Die unzureichende Reaktion auf das Ergebnis offenbart strukturelle Defizite im Umgang mit GNSS-Störungen. Daraus lässt sich wiederum ableiten, dass ein zentralisiertes Detektionssystem sowie eine klarere Zuständigkeit für PNT-Themen dringend erforderlich sind, um die Resilienz gegenüber zukünftigen Störungen zu erhöhen.

Beim autonomen Fahren werden KUUSNIEMI (2022) zufolge die Positionen des Fahrzeuges mittels absoluter und relativer Positionierung bestimmt. Zusätzlich werden andere unterstützende Systeme verwendet, ohne GNSS-Verbindung ist die Positionierung allerdings zu gefährlich und ungenau. Daraus lässt sich schließen, dass es beim autonomen Fahren zu Jamming- und Spoofing-Vorfällen kommen kann. Hierbei sind die Auswirkungen gravierend. Wenn die Fahrzeugposition nicht mehr bekannt ist, kann dies zu unsicherem Fahrverhalten führen. Dies kann wiederum zur Gefährdung der Insassen und des Umfelds führen. Insbesondere kann es zu vermeidbaren (tödlichen) Unfällen kommen, beispielhaft ist ein solcher Unfall aufgrund von Spoofing in Abbildung 4-3 dargestellt. Für automatisierte Bodenfahrzeuge in Häfen oder Flughäfen bestehen diese Gefahren ebenfalls.

Ausfälle oder Manipulationen von GNSS-Diensten stellen für autonomes Fahren eine unmittelbare Gefährdung von Menschenleben dar.



Abb. 4-3: Spoofing von autonomem Fahren
(erstellt nach KUUSNIEMI 2022)

In Unterkapitel 2.2.1 wurden weitere mögliche Anwendungen beschrieben. Im Folgenden werden daraus mögliche Auswirkungen abgeleitet. Beim beschriebenen Zielführungssystem kann der Einfluss von Jamming lediglich zum Ausfall des Systems führen, wohingegen Spoofing eine falsche eigene Position annimmt und somit die Routenführung nicht korrekt ist. Die einzige Auswirkung dabei ist, dass die anwendende Person nicht an ihr gewünschtes Ziel kommt. Beim Verkehrsleitsystem hingegen kann es als Auswirkungen bei der Störung der Koordinierung von Fahrzeugen zu Kollisionen kommen. Störungen der automatisierten Verkehrssteuerung können zu verzögerten oder fehlerhaften Entscheidungen der Leitstellen führen. Diese Auswirkungen sind nicht ungefährlich und sollten bei der Verwendung von Verkehrsleitsystemen berücksichtigt werden. Die Folgen betreffen das gesamte Systemniveau und können bei größerer Verbreitung gravierende sicherheitsrelevante Konsequenzen haben. Die Auswirkungen des Positionsmeldesystems sind identisch.

Fehlerhafte Erdbeben- und Tsunamiwarnungen können bestenfalls keine Auswirkungen haben, wenn es sich um falsch-positive handelt. Es kann aber auch bei Evakuierung der Gebiete zu potenziell hohen finanziellen Kosten kommen, aber auch zum Abstumpfen der Bevölkerung bei häufigen Fehlalarmen. Sollte es sich allerdings um falsch-negative Warnungen handeln und es steht trotz nicht vorhandener Warnung eine Naturkatastrophe bevor, kann dies weitreichende Folgen haben. Die Opferzahlen sind höher als bei möglichen Vorwarnungen. Außerdem kann es durch fehlende Alarmierung der Behörden, Bevölkerung und Einsatzkräfte zu einem größeren Chaos kommen als mit Alarmierung. Der Ausfall dieser Systeme kann allerdings auch durch andere Ursachen passieren als nur durch Jamming und Spoofing.

Im Bereich der Land- und Forstwirtschaft kann es durch Jamming und Spoofing hauptsächlich zu wirtschaftlichen Einbußen, wie mangelnden Ernteerträgen, Fehlsteuerung von Landmaschinen, Rückegassen Planung und der Zerstörung von Kulturen und Naturflächen. Diese Störungen führen zu hohen wirtschaftlichen und ökologischen Schäden. Zusätzlich kann es zur Gefährdung von Menschen und Maschine kommen, wenn plötzliche Kursabweichungen in Hanglagen oder Nachtarbeit aufgrund von GNSS-Verlust durchgeführt werden. Hier bestehen ernstzunehmende Risiken für Leib und Leben, insbesondere unter schwierigen Bedingungen.

Die aufgezeigten Beispiele verdeutlichen, dass GNSS-Störungen im Straßenverkehr, sei es durch die unbeabsichtigte oder gezielte Nutzung von PPDs, weitreichende sicherheitsrelevante, wirtschaftliche und infrastrukturelle Konsequenzen nach sich ziehen können. Während einige Anwendungen, wie einfache Zielführungssysteme lediglich funktionale Einschränkungen erfahren können. Insbesondere bei vernetzten Verkehrsleitsystemen, dem autonomen Fahren oder sicherheitskritischen Warnsystemen, können erhebliche Risiken für Menschenleben entstehen. Die Bandbreite reicht von Komfortverlust bis zu lebensbedrohlichen Auswirkungen. Je nach Anwendung ist die Resilienz gegenüber GNSS-Ausfällen zwingend sicherzustellen.

4.3.2 Auf luftgestützte Anwendungen

Im Anschluss an die Betrachtung der Auswirkungen von Jamming und Spoofing auf bodengestützte richtet sich der Fokus in diesem Unterkapitel auf luftgestützte Anwendungen, wie die Luftfahrt und Drohnen. SAALBACH (2025) zufolge ist seit September 2023 ein drastischer Anstieg von GPS-Spoofing im Luftverkehr zu verzeichnen, mit einem Höchststand von etwa 2000 betroffenen Flügen pro Tag im April 2024 (Abb. 4-4). Diese Spoofing-Vorfälle wurden oftmals durch Jamming eingeleitet (SAALBACH 2025). Sie stellen eine zunehmende Gefahr für den zivilen Flugverkehr dar. Die Zunahme der Störungen in der zivilen Luftfahrt ist sicherheitskritisch, da selbst kurzzeitige Fehlpositionierungen schwerwiegende Folgen für Flugrouten, Kollisionsvermeidung und Landeanflüge haben. Des Weiteren lassen sich potenzielle Beeinträchtigungen des Ground Proximity Warning Systems (GPWS) als kritisch betrachten. Dieses System übernimmt eine zentrale sicherheitsrelevante Funktion im Landeanflug und schützt vor dem Aufprall auf den Boden (SAALBACH 2025). Die vorliegenden Daten deuten darauf hin, dass zivile Luftfahrtsysteme derzeit in erheblichem Maß von GNSS-Störungen betroffen sind. Da diese überwiegend als unbeabsichtigte Begleiterscheinungen militärischer Operationen zu sehen sind, ist eine Besserung schwierig vorherzusagen. Diese Unvorhersehbarkeit stellt ein ernstzunehmendes Planungs- und Sicherheitsproblem für zivile Luftfahrtbetreiber dar, insbesondere in geopolitisch instabilen Regionen.



Abb. 4-4: tägliche Anzahl der gespoofen Flüge pro vorgetäuscht Gebiet (SKAI DATA SERVICES 2025b)

MEURER (2024) nennt Auswirkungen von Spoofing auf die Luftfahrt. Er stellt heraus, dass die Avionik⁷ nicht entworfen ist für Spoofing. Folgen von Spoofing sind MEURER (2024) zufolge

⁷ umfasst alle elektronischen Systeme in der Luftfahrt, dazu gehören Navigations-, Kommunikations- und Flugsteuerungssystemen (HOFFMANN o.J.)

Fehlalarme beispielsweise des Terrain Awareness and Warning Systems (TAWS) oder der Treibstoffberechnung, der Verlust von Daten wie das Wetterradar und kein sicheres Zurückkehren zum Abflugort. Außerdem muss die Flight Crew Spoofing detektieren und Gegenmaßnahmen einleiten, damit keine zusätzlichen Folgen und Gefahren entstehen. Er empfiehlt im Bereich Navigation und Kommunikation das Prinzip „Back-to-Basics“, um sich nicht von GNSS abhängig zu machen. Die hohe Komplexität der modernen Avionik führt dazu, dass Spoofing weitreichende Auswirkungen haben kann. Diese reichen von Fehlfunktionen bis hin zu sicherheitskritischen Fehleinschätzungen der Besatzung.

Die Auswirkungen von Militäroperationen und Kriegen kann man ganz deutlich in der Darstellung der gestörten und getäuschten Flugzeuge sehen. Der SKAI DATA SERVICE (2025a) visualisiert auf seiner Website diese. Auf der Website lassen sich diverse Einstellungen treffen, diese sind in den Abbildungen 4-5 bis 4-8 jeweils auf der linken Seite zu sehen. Des Weiteren kann man in der Live-Ansicht den aktuellen Stand von vor bis zu einer Stunde sehen. Außerdem lässt sich ein einzelnes Flugzeug am aktuellen Tag mittels Verlinkung zur Website www.flightradar24.com genauestens bestimmen. Die Website des SKAI DATA SERVICE (2025a) zeigt im Bereich Spoofing sowohl die Position als auch die Fluglinie vor und nach der Spoofing-Attacke (Abb. 4-5). Die Kacheln zeigen wie auch bei WISEMANN (2022) die Jamming-Wahrscheinlichkeit der Flugzeuge an. Weitere Funktionen sind auf der Website von SKAI DATA SERVICE (2025a) zu finden. Die folgenden Abbildungen zeigen, dass der Russland-Ukraine Krieg und der Israel-Iran Konflikt aktuell einige Auswirkungen auf die Luftfahrt haben. In der Abbildung 4-7 ist ein Gesamtüberblick vom 09.06.2025 zu sehen, wenn man diesen mit dem identischen Ausschnitt (Abb. 4-8) vom 15.06.2025

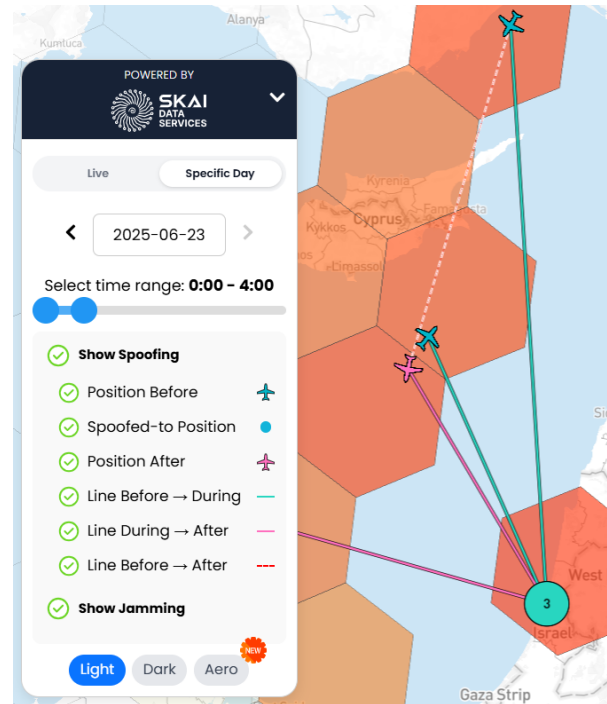


Abb. 4-5: Spoofing eines Flugzeuges
(SKAI DATA SERVICES 2025a)

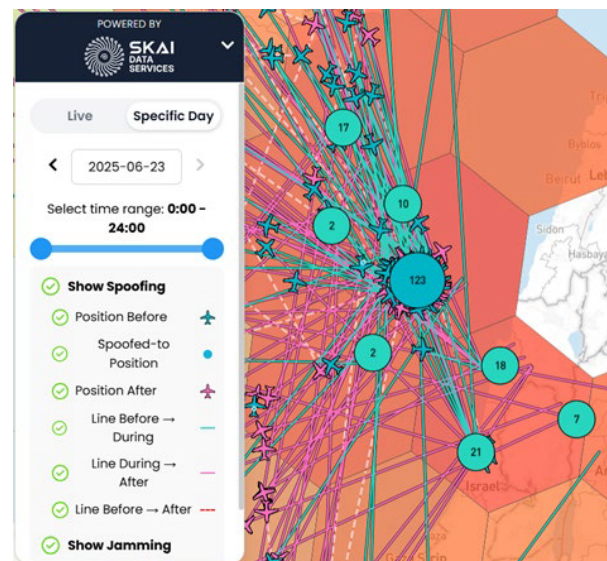


Abb. 4-6: Zoom auf Ballungsraum Naher Osten
(SKAI DATA SERVICES 2025a)

vergleicht, ist deutlich ein Anstieg der Störungen im Bereich des Nahen Ostens zu sehen. Dies ist auf den israelischen Angriff auf den Iran zurückzuführen. Des Weiteren kann man in diesen beiden Abbildungen starke Störungen im Bereich Osteuropa und Ostseeraum erkennen. Dies lässt wiederum Rückschlüsse auf unter anderem den Balic Jammer (vgl. 4.3.3) zu. Beim Zoom an den Stör-Hotspot (Abb. 4-6) im Nahen Osten fällt auf, dass der Ballungsraum für Spoofing vor der Küste Israels liegt. Dies beschreibt einen guten Fall von untargeted Spoofing. Vermutlich wurde dieses verwendet, da es weniger Leistung als Jamming benötigt. Die kartographische Darstellung verdeutlicht, dass GNSS-Störungen zunehmend gezielt zur strategischen Luftraumkontrolle eingesetzt werden und dies globale Auswirkungen auf die zivile Luftfahrt hat.

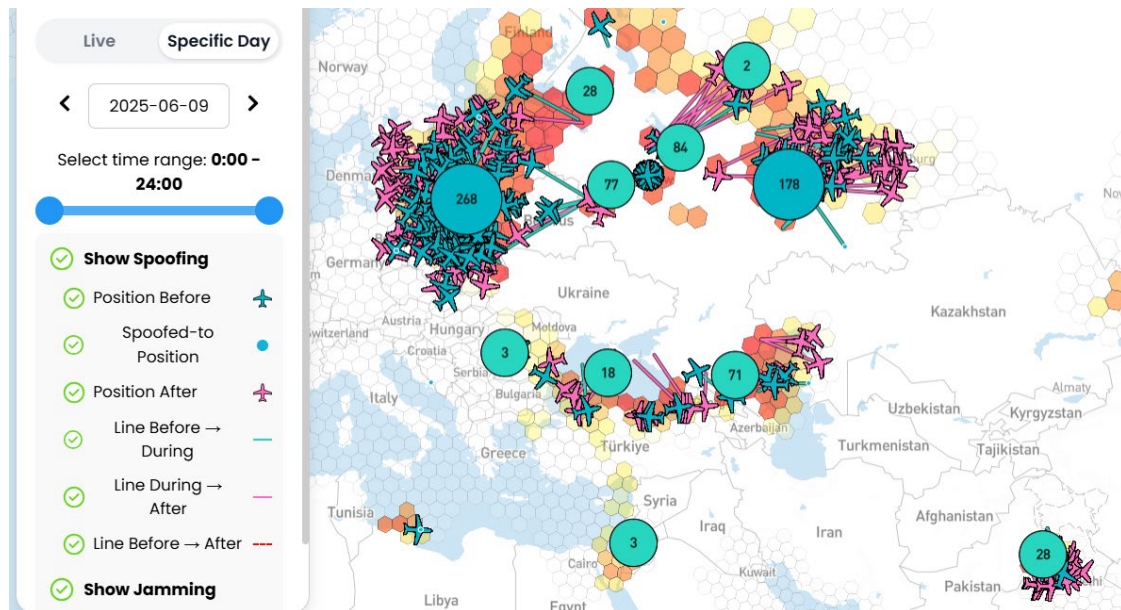


Abb. 4-7: Jamming und Spoofing auf Flugzeuge am 09.06.2025 (SKAI DATA SERVICES 2025a)

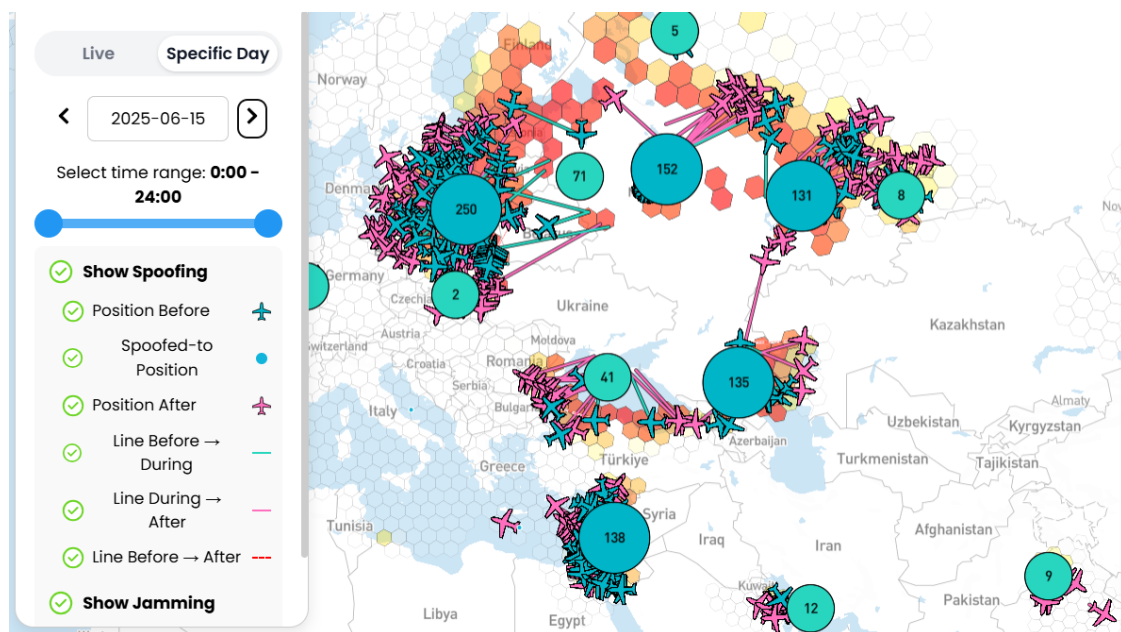


Abb. 4-8: Jamming und Spoofing auf Flugzeuge am 15.06.2025 (SKAI DATA SERVICES 2025a)

RETERSKI (2015) äußert sich treffend zu den Auswirkungen. Er sagt, dass die zivile Luftfahrt weiterhin GNSS-Störungen erleben wird und möglicherweise auf robustere verschlüsselte Systeme umsteigen muss. In Entwicklungsländern könnte laut ihm GNSS das Standard-Navigationsmittel für die Luftfahrt bleiben, dies stellt allerdings ein gerngesehenes Ziel für böswillige Akteure dar. Länder mit fortschrittlicher Infrastruktur hingegen sollen die Navigation mit erhöhter Geschwindigkeit, Zuverlässigkeit und Redundanz verbessern. Der technologische Unterschied zwischen entwickelten und weniger entwickelten Staaten führt zu global ungleichen Resilienzen gegenüber GNSS-Störungen mit sicherheitspolitischer Relevanz.

Auch der Themenkomplex Loitering Munition hat mit den Auswirkungen durch Störsender zu kämpfen. Bei Loitering Munition handelt es sich um Flugkörper, die mithilfe eines eigenen Antriebes in einen Einsatzraum fliegen und dort eine gewisse Zeit in der Luft kreisen (KATHER et al. 2025). Sie erkennen ihr Ziel eigenständig und übergeben diese Information an den Bediener. Dieser entscheidet über das weitere Vorgehen in Form der Bekämpfung. Zusätzlich zur GPS-Steuerung kann auch die von der Führung benötigte Telemetrieübertragung gestört werden. (NAGY 2024). Auch wenn Loitering Munition als Kamikazedrohnen bezeichnet wird, sind diese keine Drohnen, da es sich hier um Munition



Abb. 4-9: Abschuss von Loitering Munition
(UNMANNED NETWORK 2023)

handelt, die für den einmaligen Abschluss (Abb. 4-9) hergestellt wird (KATHER et al. 2025). Trotz dessen lassen sich die abgeleiteten Auswirkungen der Störsender auf Kamikazedrohnen sehr mit denen der Drohnen vergleichen. Keine GNSS-Verbindung bedeutet zwangsweise keinen Einsatz von Loitering Munition. Die GNSS-Abhängigkeit dieser Waffensysteme macht sie im elektromagnetischen Spektrum angreifbar und reduziert ihre Einsatzsicherheit erheblich, was potenziell strategische Konsequenzen haben kann.

Dieses Unterkapitel verdeutlicht, dass Jamming und Spoofing im luftgestützten Anwendungsbereich weitreichende sicherheitsrelevante, operationelle und geopolitische Konsequenzen nach sich ziehen können. Es macht außerdem klar, dass der passende Umgang mit diesen Störungen essenziell in der Zukunft sein wird, da immer mehr GNSS-Störungen auftreten. Angesichts der steigenden Zahl und Intensität von Vorfällen ist ein international koordiniertes Maßnahmenpaket zur Erkennung, Abwehr und strukturellen Prävention von GNSS-Störungen im Luftfahrtbereich dringend geboten.

4.3.3 Auf maritime Anwendungen

Die Verwendung von beabsichtigten Störsendern kann in der Schifffahrt zu erheblichen Risiken führen. Besonders in stark befahren oder engen Gewässern kann der Verlust präziser Positionsdaten weitreichende Folgen haben. WESTBROOK (2019) zufolge können Störsender Schiffpositionsdaten um bis zu 10m beeinflussen. Bei einem Vorfall, den er nennt, kam es aufgrund einer GPS-Störung zur Kollision zweier großer Schiffe in der Kieler Förde. Anhand dessen lässt sich die Relevanz dieser Bedrohung im zivilen Bereich unterstreichen. Die enge Nähe von Schiffen in vielbefahrenen Gewässern macht die genaue Positionsbestimmung überlebenswichtig, weshalb GNSS-Störungen hier direkt die Schifffahrtssicherheit und damit Menschenleben gefährden können.

Eine weitere Bedrohung und Auswirkung auf den Schiffsverkehr stellt der koordinierte Einsatz einzelner oder mehrerer Geräte, wie beispielsweise PPDs, insbesondere in hochfrequentierten Regionen wie dem Ärmelkanal da (WESTBROOK 2019). Aufgrund seines Artikels lässt sich beurteilen, dass die Nutzung der PPDs immer gefährlicher für den Schiffsverkehr wird, sei es bei schwerwiegenden Schifffahrtsunfällen oder allgemein bei der Navigation der Schiffe.

Gerade auch der koordinierte Einsatz von Jammern stellt eine steigende Bedrohung dar und birgt stärkere Risiken durch den Anstieg der Nutzung in den letzten Jahren. Des Weiteren lässt sich sagen, dass es unterschiedliche Auswirkungen auf die Schifffahrt in binnen- oder internationalen Gewässern gibt, da sich die Verkehrsdichte in diesen Gebieten stark unterscheidet. Diese Entwicklung erfordert eine verstärkte Regulierung und Kontrolle von Störsendern sowie die Entwicklung widerstandsfähigerer Navigationssysteme, um die Risiken für maritime Sicherheit zu minimieren.

Im Bereich der Container-Überwachung wird ebenfalls GNSS eingesetzt. RETERSKI (2015) nennt Möglichkeiten, wie dies mittels Jamming und Spoofing ausgenutzt werden kann. Durch die Nutzung von Störsendern lassen sich unbemerkt die Positionen von Containern in Hafen verändern, somit ist ein Diebstahl möglich, ohne dass sich die Position ändert. Aus seinem Bericht lassen sich verschiedene Auswirkungen der Container-Überwachung herausstellen. Ein Diebstahl kann weitreichende Auswirkungen haben, je nach Ladung. Jammer stellen nicht nur eine Bedrohung für den Versandkunden dar, sondern auch für den umliegenden Verkehr im Logistikzentrum und Hafen, hier kann es zu Kollisionen kommen. Die Manipulation von Containerpositionen gefährdet die Sicherheit und Integrität globaler Lieferketten, führt zu wirtschaftlichen Verlusten und erhöht das Risiko von Unfällen in Hafenanlagen.

Spoofing-Angriffe bergen die Gefahr gezielter Kursabweichungen, was sicherheits- und handelspolitische Konsequenzen haben kann. Besonders besorgniserregend ist dabei der Umstand, dass die Nutzer möglicherweise nicht erkennen, dass sie fehlerhafte Navigationsdaten empfangen. Ein Beispiel für eine Kursabweichung des Containerschiffs „SKALAR“ (KPLER 2025), dessen GNSS-Positionen in Abbildung 4-10 zu sehen sind. Es handelt sich um Positions-Spoofing durch fremdes Einwirken. Hier wurden zwei verschiedene Ausschnitte vom 14.06.25 (Abb. 4-10 oben) und 15.06.25 (Abb. 4-10 unten) gezeigt. Auf dem Ausschnitt vom 14.06.25 ist ein erster Positionssprung zu sehen. Die SKALAR befindet sich zu dem Zeitpunkt auf der nördlichen Seite der Insel und nicht wie dargestellt am Festland. Auf dem zweiten Ausschnitt sind einige Positionssprünge des Containerschiffs zu sehen.

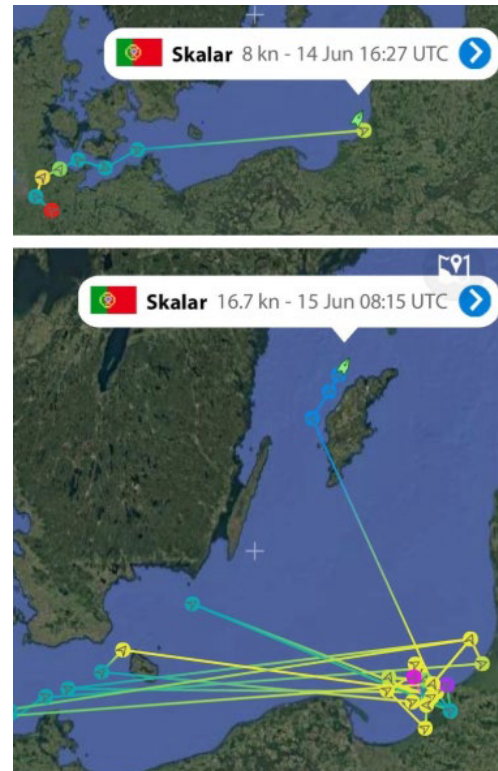


Abb. 4-10: Kursabweichung durch Spoofing
(KPLER 2025)

WESTBROOK (2019) nennt ein Beispiel, bei dem die fehlerhafte PNT-Information sehr schnell erkannt werden konnte. In diesem Fall befanden sich 20 Schiffe, anstatt im Schwarzen Meer, ungefähr 20 Seemeilen landeinwärts. Hier ist offensichtlich, dass diese Informationen nicht korrekt sein können, dementsprechend gab es auch keine Auswirkungen, da auf alternative Navigationsmöglichkeiten umgestellt wurde.

Seit der russischen Invasion 2022 gab es vermehrt Vorfälle (Abb. 4-11) von GNSS-Störungen im Ostseeraum, dazu äußert sich KIESEWETTER (2024) in seiner Analyse und wird für diesen Abschnitt als Literatur verwendet. Ein medial 2024 sehr großes Thema war der Baltic Jammer. Details zu diesem Thema sind zu weitreichend für den Umfang dieser Bachelorarbeit. Vermutlich handelt es sich um ein sehr komplexes Störsystem mit diversen Technologien. Der genaue Standort des Jammers ist bisher nicht geklärt, die Beweislage geht aber stark von Kaliningrad aus. Die Störungsentfernungen reichen über die gesamte Ostsee, insbesondere von Polen und dem Baltikum bis nach Südschweden und Nordostdeutschland.

Des Weiteren steht der Baltic Jammer im Zentrum der Vorwürfe, was die aktuellen Jamming-Vorfälle in diesem Bereich angeht. Er führt neben technischen Auswirkungen auch zu erheblichen gesellschaftlichen Auswirkungen. Auch die in Abbildung 4-10 dargestellte Kursabweichung lässt sich sehr wahrscheinlich darauf zurückführen. Dieser Vorfall illustriert, wie politische Konflikte GNSS als Ziel für hybride Kriegsführung nutzen und dadurch die regionale Stabilität und zivile Sicherheit gefährden.

Die GPS-Interferenz im Bereich der Ostsee zum Zeitpunkt des aktiven Baltic Jammers ist in Abbildung 4-11 zu sehen. Auf der dazugehörigen Website von WISEMANN (2022) werden die Genauigkeiten der Navigationssysteme der Flugzeuge dargestellt. Es muss sich hierbei nicht zwingend um Jamming handeln, die Wahrscheinlichkeit ist allerdings sehr hoch, gerade wenn ein Jammer zu dem Zeitpunkt im Einsatz ist. Des Weiteren ist zu beachten, dass je mehr Flugzeuge über eine Route fliegen desto aussagekräftiger ist die der Kachel zugeordneten Wahrscheinlichkeit. Die Kacheln zeigen die

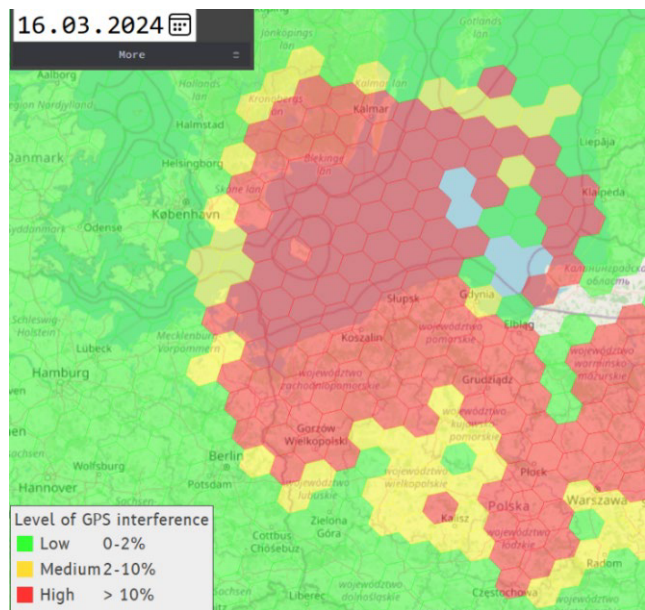


Abb. 4-11: GPS-Interferenz im Ostseeraum
(WISEMANN 2022)

gemeldeten Interferenzen der dort geflogenen Flugzeuge in Prozent. Die Auswirkungen von Jamming auf den Luftverkehr, welche im Unterkapitel 4.3.2 erläutert wurde, im Einzugsbereich maritimer Routen zeigt die komplexen Wechselwirkungen zwischen verschiedenen Verkehrsträgern und macht die Vernetzung der Sicherheitsmaßnahmen unerlässlich.

Neben den durch Andere hervorgerufene Spoofing-Fälle gibt es auch selbst herbeigeführte Täuschungen der eigenen Position durch Schiffsbetreiber oder -systeme. Diese stellen ebenfalls eine weitere Gefahrenquelle dar. Dadurch kann es laut WESTBROOK (2019) zu unabsichtlichen Fehlleitungen kommen, wenn etwa fehlerhafte GNSS-Empfänger oder falsch konfigurierte Navigationssysteme das Signal manipulieren. Hierbei kann es zu falschen Positionen und gefährlichen Kursabweichungen kommen. Zusätzlich berichten BERGMANN et al.(2023) berichtet von der Fälschung der eigenen AIS-Daten durch Spoofing. AIS-Systeme nutzen GNSS zur Positionierung. Das ursprünglich zur Kollisionsvermeidung entwickelte System kann ebenfalls zum Nachvollziehen von Positionen verwendet werden (BERGMANN et al. 2023).

Der Bericht enthält eine Analyse zum Thema systematisch manipulierte AIS-Positionsdaten, um den tatsächlichen Aufenthaltsort in russischen Schwarzmeerhäfen zu verschleiern. In diesem Fall geht es um vier Öltanker, die trotz internationaler Sanktionen gegen Russland an diesen Häfen angelegt haben. Laut AIS-Daten befanden diese sich bis zu mehreren hundert Seemeilen vom Hafen entfernt. Es kam durch die Kombination aus satellitengeschützten Radaraufnahmen (Abb. 4-12) und übermittelten Bewegungsdaten (Abb. 4-13), zur Überführung der Fehlpositionierung (vgl. 5.1) (BERGMANN et al. 2023). Die Erklärung eines exakten Beispiels kann den Abbildungen 4-12 und 4-13 entnommen werden.

Aus der Analyse von BERGMANN et al. 2023 lässt sich ableiten, dass diese Art des Spoofings immer weiter zunimmt und gerade im Kontext des Ukrainekrieges das Täuschen der eigenen Position relevanter geworden ist. Zudem wird hier die Ausbreitung und Bedrohung des Spoofing-Phänomens auch auf kommerzielle und geopolitische Ebenen verdeutlicht.

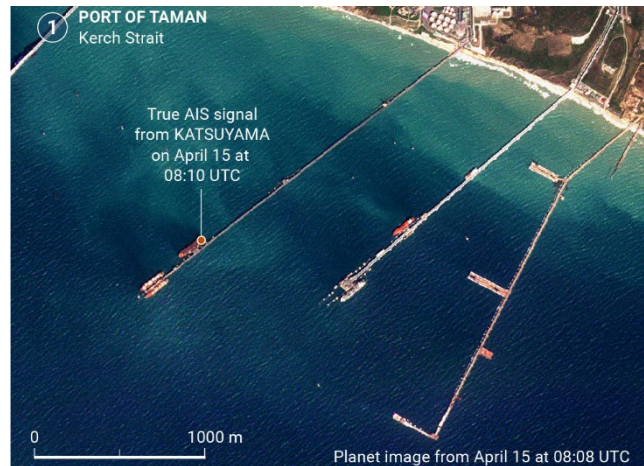


Abb. 4-12: Satellitenaufnahmen (BERGMANN et al. 2023)

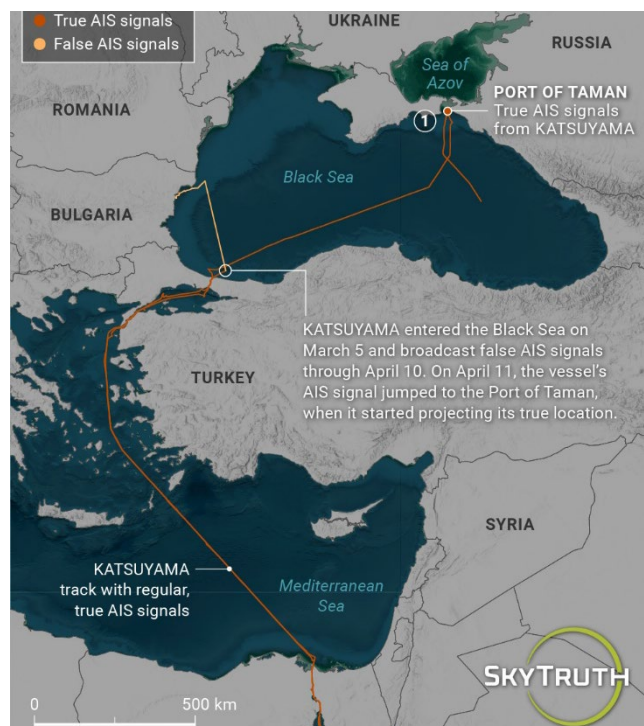


Abb. 4-13: AIS-Signale und Bewegungsdaten (BERGMANN et al. 2023)

Außerdem wird aus der Analyse deutlich, dass Spoofing eine erhebliche Herausforderung für die maritime Überwachung und die Durchsetzung internationaler Normen und Gesetze darstellt. Daraus ergibt sich die Notwendigkeit zur Prüfung der Authentizität von Positionsinformationen durch robuste, mehrschichtige Detektionsmechanismen (vgl. 5.1), Sensorfusion und unabhängige Satellitenbilddaten kombinieren. Diese Entwicklungen zeigen, dass Spoofing zu einem strategischen Werkzeug im geopolitischen Machtspiel geworden ist und zwingt Staaten sowie Organisationen zu verstärkten Investitionen in Sicherheit- und Überwachungstechnologien.

GNSS-Spoofing kann laut RETERSKI (2015) neben der Kursabweichung zur illegalen Überfischung genutzt werden, deren Wert weltweit auf mehr als 23 Milliarden US-Dollar pro Jahr geschätzt wird. Gelingt das Spoofing der eigenen Position könnte auf diese Weise eine Flotte von Fischereischiffen in Meeresschutzgebiete einfahren, ohne ihre Transponder auszuschalten und die Aufmerksamkeit von Kontroll- und Überwachungssystemen zu erhalten. In ähnlicher Weise können auch Besatzungen, die Schmuggel und Menschenhandel betreiben, Spoofing nutzen, um ihre Routen zu verschleiern (RETERSKI 2015). Dementsprechend hat das gezielte Täuschen der eigenen Position meist einen kriminellen Gedanken, die Auswirkungen lassen sich je nach Szenario differenzieren. Es geht hierbei häufig um finanzielle Profite, welche durch das Spoofing erhöht werden können. Diese Form des Spoofings gefährdet nicht nur die maritime Sicherheit, sondern fördert auch illegale Aktivitäten mit erheblichen wirtschaftlichen und gesellschaftlichen Folgen. Dies verdeutlicht die Notwendigkeit umfassender Überwachung und Durchsetzung von Gesetzen.

Die meisten zu schlussfolgernden Auswirkungen durch Jamming und Spoofing der zusätzlich in Unterkapitel 2.2.3 genannten Anwendungen, wie die Bestimmung der Meerestiefe oder der Meeresbodenstruktur, die Aktualisierung von Seekarten und die Positionierung von Offshore-Fahrzeugen sind eindeutig. Beim Verlust der GNSS-Verbindung ist eine Bestimmung der Meerestiefe sowie der Meeresbodenstruktur nicht mehr möglich. Es muss ein erneuter Vermessungstermin angesetzt werden, dies hat lediglich finanzielle Auswirkungen im Regelfall sollte es keine Störungen anderer, Personen-, Materialschäden oder Ähnlichem. geben.

Die fehlerhafte Aktualisierung von Seekarten kann wiederum zu Fehlern durch den Kartenlesenden kommen und dies kann je nach gewünschter Anwendung neben Gefährdungen des Schiffes zu Umweltkatastrophen, Verzögerungen im Schiffsverkehr, aber auch zu wirtschaftlichen Verlusten kommen. Zudem besteht Gefahr für Leib und Leben, da Schifffahrtshindernisse in Seekarten verzeichnet sind und falsche Karten zum Kentern führen können.

Ähnliche Auswirkungen kann der Verlust der GNSS-Verbindung für Offshore-Fahrzeuge haben. Zusätzlich kann es zu Verzögerungen im Bau- und Wartungsablauf, zum Ausfall von automatisierten Systemen, aber auch zur Beeinträchtigung von Sicherheitsoperationen wie Notfalleinsätzen oder Evakuierungen kommen. Die Auswirkungen zeigen, dass Jamming und Spoofing nicht nur akute Sicherheitsrisiken mit sich bringen, sondern auch mittel- und langfristige operative sowie wirtschaftliche Nachteile hervorrufen, die insbesondere in sensiblen Bereichen gravierend sein können.

5 Störungsmanagement

Um die im vorherigen Kapitel dargelegten Auswirkungen und Gefahren von Jamming und Spoofing auf zivile, militärische, boden-, luftgestützte und maritime Anwendungen zu minimieren, wird in diesem Kapitel der Umgang mit Bedrohungen analysiert. Zunächst wird auf mögliche Verfahren zur Detektion von Jamming und Spoofing eingegangen, gefolgt von möglichen Gegenmaßnahmen. Abschließend werden verschiedenen alternativen Navigationsansätze dargestellt, um eine Robustheit gegenüber GNSS-Störungen zu erhöhen.

5.1 Detektion von Jamming und Spoofing

Die frühzeitige Erkennung von absichtlichen Störungen ist eine zentrale Voraussetzung für einen sicheren und robusten Betrieb GNSS-gestützter Anwendungen. Ziel ist es, Störungen zuverlässig zu identifizieren, deren Ursprung und Charakter zu bestimmen und somit eine fundierte Grundlage für nachfolgende Gegenmaßnahmen (vgl. 5.2) zu schaffen.

BAUER (2017) differenziert die Methoden der Erkennung von Störungen in Prä- und Postkorrelation (vgl. 2.1). Die Beschreibung dieser Methoden erfolgt auf Basis von BAUER (2017). Bei der Präkorrelation handelt es sich um Front-End-Auswertungen, hier ergeben sich wiederum zwei Möglichkeiten der Suche nach Interferenzen. Entweder die Suche erfolgt während oder nach der Digitalisierung (vgl. 2.1).

Bei der Suche während der Digitalisierung gibt es die Möglichkeit der Überwachung der Signalstärken. Da GNSS-Signale in der Regel schwächer sind als das Noise Floor des Empfängers, kann davon ausgegangen werden, dass es sich um eine Störung handelt, sobald ein Signal empfangen wird, was deutlich über diesem Pegel liegt. Bei der Signalverarbeitung werden in Stufen

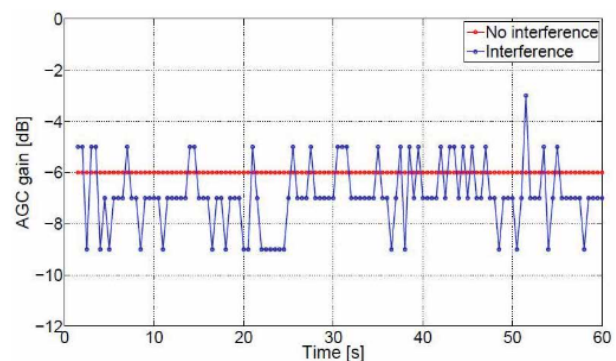


Abb. 5-1: Veränderung der Signalstärke durch AGC (BAUER 2017)

gemessene Signalstärken mit einem Schwellenwert verglichen, bei dessen Überschreitung von einer Störung des Signals ausgegangen werden kann. Dies ist besonders für die Detektion von Störsignalen geeignet, die über ein konstantes Leistungsdichtespektrum mit weißem Gauß-Signal verfügen. Ein weiterer Ansatz der Suche während der Digitalisierung ist das Monitoring der Automatic Gain Control (AGC), also der automatischen Verstärkungsregelung im Empfänger. Bei ungestörten GNSS-Signalen bleibt der Verstärkungsbedarf nahezu konstant. Tritt jedoch ein starkes Störsignal auf, steigt der Signalpegel und die AGC reduziert die Verstärkung entsprechend. Plötzliche und ungewöhnliche Absenkungen der Verstärkungswerte deuten auf eine Signalstörung hin, dies ist in Abbildung 5-1 dargestellt.

Bei der Suche nach der Digitalisierung nennt BAUER (2017) zu Beginn die Suche durch Analyse der Analog-digital-Wandlung. Diese Möglichkeit ergibt sich aus den unterschiedlichen statistischen Eigenschaften eines ungestörten und eines gestörten Empfangssignals sowie den Eigenschaften des Analog-Digitalwandlers. Die Amplituden der digitalisierten ungestörten Signale entsprechen einer gaußschen Normalverteilung. Durch die Erstellung eines Histogramms der digitalisierten Signalamplituden und die Analyse, ob dies eine Normalverteilung darstellt, können gestörte GNSS-Signale aufgespürt werden. Bei der Erstellung ist auf die Auflösung des ADCs zu achten, da sich die Histogramme unterscheiden.

Im Anschluss nennt BAUER (2017) die Suche durch Spektralanalysen mithilfe einer Fast-Fourier-Transformation (FFT). Dabei wird das empfangene Zeitsignal mathematisch in den Frequenzbereich überführt, um charakteristische Frequenzkomponenten sichtbar zu machen. Abweichungen vom erwarteten Frequenzspektrum insbesondere das Auftreten zusätzlicher Störfrequenzen deuten auf Interferenzen hin. Außerdem lassen sich die Frequenzen des Störsignals herausfinden und die Störsignale im Anschluss mit einer geeigneten Methode filtern oder dämpfen. Eine genauere Beschreibung der Transformation würde hier den Rahmen dieser Arbeit sprengen. REISNER (2024) nennt diese Form der Jamming-Detektion ebenfalls. Im Ukrainekrieg werden vom Drohnenoperator Spektrumanalysatoren verwendet, um sowohl Belastungen durch Jamming von gegnerischen Kräften als auch Bewegungen im Frequenzbereich der Drohnen zu detektieren. Die Erfolgchancen dieser Detektionsart im Kampfeinsatz, lässt REISNER (2024) allerdings offen.

Bei der Postkorrelation, also der Auswertung im Basisbandprozessor unterscheidet BAUER (2017) ebenfalls in zwei Ansätze. Die erste ist die Überwachung der Signalqualität. Wie bereits in Unterkapitel 2.1 beschrieben, eignen sich für die Beschreibung der Signalqualität die Signal-to-Noise Ratio (SNR) und die Carrier-to-Noise Density Ratio (C/N_0) (BAUER 2017). Die meisten Empfänger geben Werte für den als letztes genannten Indikator, weshalb dieser im Folgenden betrachtet wird. Ein Parameter, welches im Bereich Interferenzen genutzt wird, ist der effektive C/N_0 -Wert. Dieser wird laut BAUER (2017) durch die Formel 5-1, welche sich aus dem C/N_0 -Wert und der existierenden Interferenz I zusammensetzt. Aufgrund dessen, dass verschiedene Arten der Bestimmung des Wertes existieren, können keine Schwellwerte angegeben werden, ab wann eine signifikante Störung vorliegt. Die wichtigste Erkenntnis dabei ist, dass der C/N_0 durch Interferenzen kleiner wird.

$$\left(\frac{C}{N_0}\right)_{eff} = \frac{C}{N_0 + I}$$

Formel 5-1: effektiver C/N_0 -Wert (BAUER 2017)

Die zweite Methode der Postkorrelation ist die Überwachung der Korrelatorwerte bei Multikorrelator-Empfängern. Wie bereits erklärt, schätzen GNSS-Empfänger die Pseudostrecke durch Korrelation des empfangenen Signals mit einer lokal im Empfänger erzeugten Signalnachbildung. Herkömmliche Empfänger verfügen meist über drei Korrelatoren. Multikorrelator-Empfänger verfügen über deutlich mehr als drei Korrelatoren und ermöglichen es die Korrelationswerte des reinkommenden Signals mit der pünktlichen, diversen verfrühten und verspäteten Signalnachbildungen zu vergleichen. Moderne GNSS-Empfänger verfügen über bis zu 100 Korrelatoren. Bei Störungen durch CW-Jamming verändert sich die typische Form der Korrelatorfunktion (Abb. 5-2). Sie wird von einem sichtbaren Sinus-Cosinus-Signal überlagert. Die Amplitude der Überlagerung hängt dabei von der Frequenz und der Leistung des Störsignales ab. Durch Anwendung der FFT auf das Korrelationssignal lassen sich Jamming-relevante Parameter wie Frequenz, Amplitude und Bandbreite des Störsignals ableiten.

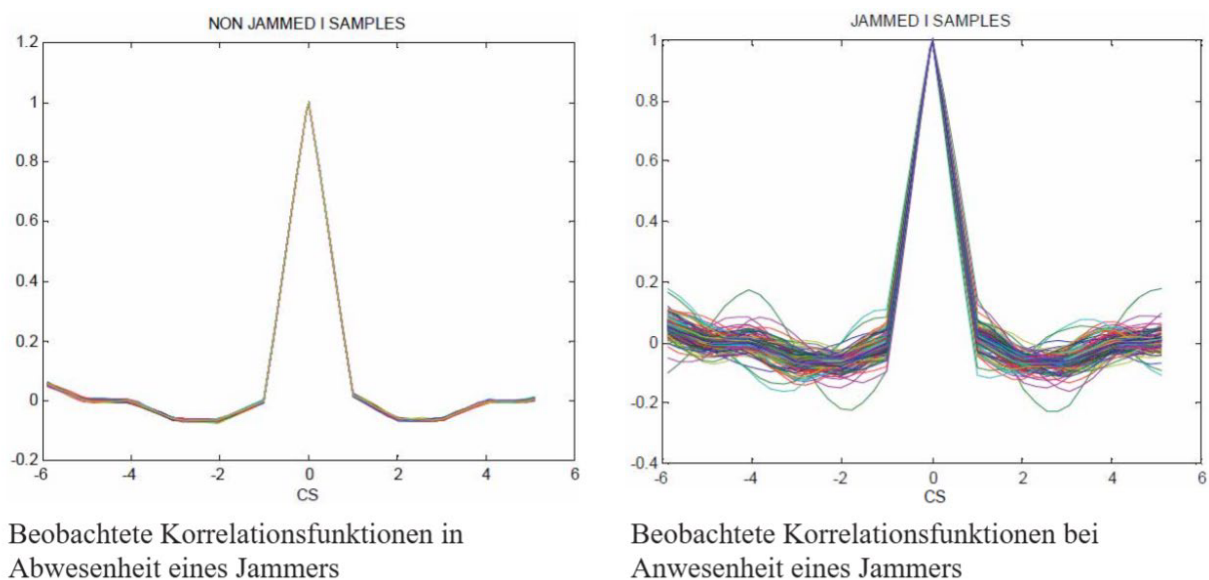


Abb. 5-2: Veränderung der Korrelationsfunktion durch Jamming (BAUER 2017)

CLEMENTS et al. (2023) erforscht die Detektion mittels Low Earth Orbit (LEO) Satelliten. LEO-Satelliten sind aufgrund ihrer Position besonders geeignet terrestrische GNSS-Störsender zu detektieren, klassifizieren und zu lokalisieren. In der Analyse werden zwei Möglichkeiten der Nutzung dieser Satelliten beschrieben. Die direkte Geolokalisierung basiert auf einer einstufigen Suche über ein geografisches Raster bei der die Position des Störsenders unmittelbar aus dem empfangenen Signal geschätzt wird. Die konventionelle zweistufige Geolokalisierungsmethode hingegen schätzt erst die differentielle Laufzeitverzögerung und den differentiellen Dopplereffekt. Danach wird der Standort des Störsenders anhand der zeitlichen Entwicklung dieser Parameter berechnet. Der direkte Ansatz liefert auch bei einem niedrigeren SNR und kurzen Aufzeichnungszeiten mit mehreren Störquellen eine effektive Detektion. Außerdem ist hiermit die Geolokalisierung mehrerer Störsender mit zyklstationären Signalen, wie bei Chirp-Jammern, möglich. Mit der zweistufigen Methode ist es hingegen schwer diese Signalarten zu

detektieren und die einzelnen Sender können nicht den entsprechenden beobachteten Strukturen der Differenzverzögerungen und -dopplerfrequenzen zugeordnet werden.

Zur Detektion von Spoofing nennt BLUM (2022) die Doppler-Frequenzverschiebung, welche dem Basisbandprozessor entnommen werden können. Es ergibt sich je nach Satellit eine andere Variation der Doppler-Frequenzverschiebung pro Zeit, da die authentischen GNSS-Signale aus verschiedenen Richtungen mit verschiedenen Entfernungen kommen. Da beim Spoofing nur ein Störsender verwendet wird, kommen hier alle Spoofing-Signale aus einer Richtung und mit der gleichen Entfernung. Der unterschiedlichen Verläufe der Doppler-Frequenzverschiebungen je Zeit sind in Abbildung 5-3 zu sehen, wobei a) die authentischen GNSS-Signale und b) die Spoofing-Signale darstellt.

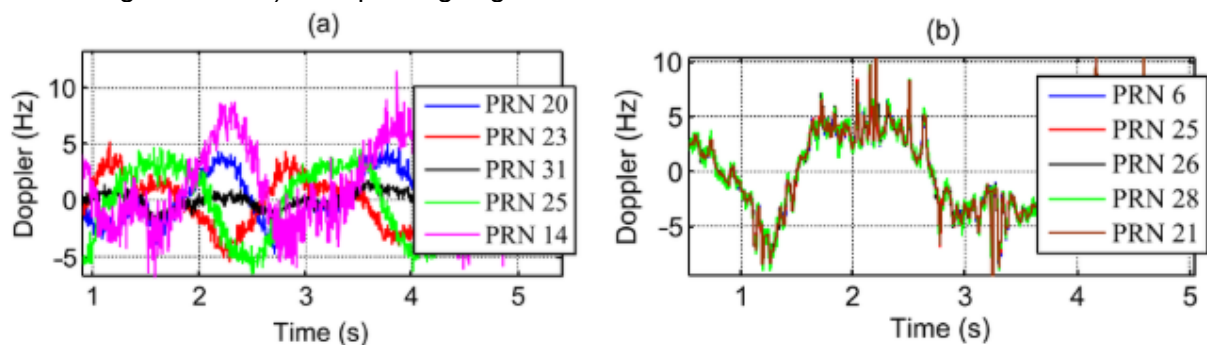


Abb. 5-3: Verlauf der Doppler-Frequenzverschiebung mit und ohne Spoofing (BLUM 2022)

Es werden aufgrund der deutlichen elektromagnetischen Signatur des Jammers auf dem Gefechtsfeld von morgen passive Möglichkeiten zur Detektion von Drohnen benötigt (NAGY 2024). Es wird als Beispiel eine rein passive Radiofrequenzdetektion vorgeschlagen, da diese nicht abstrahlt und einen geringen Stromverbrauch aufweist. Eine Möglichkeit, die bereits im Ukrainekrieg verwendet wird, sind Lichtwellenleiter als emissionslose Steuermethode der Drohnen. Hierbei wird jegliche elektromagnetische Signatur vom gesamten Drohnenkomplex inklusive Bodenstation reduziert.

Allgemein lässt sich sagen, dass große Störsender mit hoher Sendeleistung attraktive Ziele im militärischen Kontext sind, die kleineren lassen sich hingegen schwerer orten und erfordern Schutzmaßnahmen wie verbesserte Anti-Jamming-Technologien im Empfänger, verbesserte Antennen oder die Integration von Ergänzungssystemen (Schmidt 2013). Militärische Jammer sind aufgrund ihrer größeren elektromagnetischen Strahlung besser zu detektieren (FINK 2013). Hingegen kann es WESTBROOK (2019) zufolge einige Zeit in Anspruch nehmen, bis mehrere kleine PPDs im urbanen Raum Jamming-Quellen aufgefunden und ausgeschaltet sind. Wenn ein Spot beam verwendet wird, erhöht sich die Detektionsmöglichkeit laut MÜLLER (2008) um ein Vielfaches. Ein weiteres Indiz, dass eine bewusste Signalstörung vorliegen kann, ist es, wenn mehrere Empfänger unabhängiger Hersteller kein Signalempfangen können (CISA 2022).

Im Fall der Öltanker, die an russischen Häfen angelegt haben, erfolgte die Spoofing-Enttarnung durch die Kombination mehrerer Technologien (TRIEBERT et al. 2023). Es wurden wie beschrieben die satellitengestützten Radaraufnahmen ausgewertet, welche keine Schiffe zeigten. Zum gleichen Zeitpunkt erhielten AIS-Empfangsstationen manipulierten Signale. Die Bewegungsdaten zeigten zusätzlich unplausible Muster, wie das vollständige Fehlen des Treibens bei angeblich stillliegenden Schiffen oder abrupte Ortswechsel ohne erkennbare Ursache.

Zur Lokalisation von Störsendern muss BLUM (2022) zufolge ein Überwachungssystem aus mindestens drei Monitorstationen und einem damit in Kontakt stehendem Kontrollzentrum bestehen. Die Monitorstationen müssen Störungen detektieren und die Entfernungen oder Richtungen des Störsenders bestimmen können. Zur Ermittlung der Entfernung können die Differenzen der Ankunftszeiten der Störsignale bei den verschiedenen Monitorstationen ermittelt werden. Für die Richtungsermittlung können adaptive Antennengruppen verwendet werden. Die Position des Störsenders lässt sich im Kontrollzentrum mittels Entfernungen oder Richtungen von mindestens drei Empfängern zu einer Störquelle berechnen.

Eine Möglichkeit zur Lokalisation von Störsendern ist die künstliche Intelligenz basierte Detektion (Abb. 5-4) (GEWIES et al. 2024). Dabei wird sich auf die Nutzung von GNSS-Rohdaten beschränkt. Hierbei werden beim Jamming die bereits erläuterten Indikatoren ADC , C/N_0 -

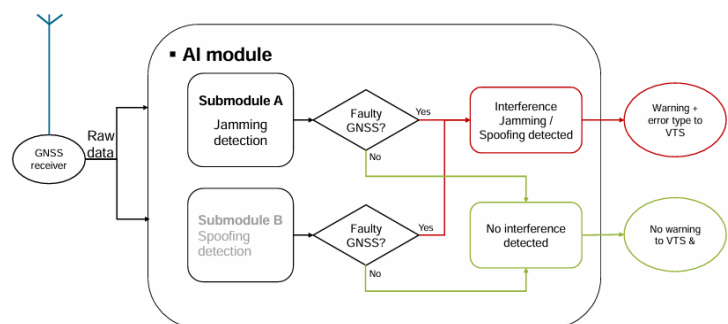


Abb. 5-4: Künstliche Intelligenz basiertes Detektionschema von Jamming und Spoofing (GEWIES et al. 2024)

Wert und die Anzahl der erfassten Satelliten verwendet. Zusätzlich wird beim Spoofing die gemessenen Stationskoordinaten mit den GNSS-Positionen verglichen und ein Multi-Antennensetup verwendet, um eine Basislinienbestimmung durchzuführen.

RETERSKI (2015) nennt einen Lösungsansatz zur Erkennung und Schwarmlokalisierung von GNSS-Störungen. Dabei schlägt er vor, das bestehende Mobilfunknetz als verteiltes Detektionssystem zu nutzen. Durch die Integration einer einfachen nicht näher beschriebenen Zusatzkomponente in neu produzierten Mobiltelefonen, könnten dichte Mobilfunknetze, vor allem in urbanen Regionen, zur passiven Erfassung, Messung und Meldung von GNSS-Signalstörungen herangezogen werden. Die gesammelten Daten würden an eine zentrale Überwachungseinheit übermittelt werden, die daraus eine räumliche Darstellung des Störgebietes sowie eine Lokalisation der Störquelle ableiten könnte. Unklar bleibt jedoch, ob der rechtliche Rahmen eine solche passive Nutzung von privaten Endgeräten für staatliche Detektionszwecke zulassen würde.

5.2 Schaffen von robustem GNSS

Nachdem im vorangegangenen Unterkapitel die unterschiedlichen Verfahren zur Detektion von Jamming- und Spoofing beschrieben wurden, widmet sich das folgende Unterkapitel den möglichen Gegenmaßnahmen. Während die frühzeitige Erkennung solcher Störungen eine grundlegende Voraussetzung für den Schutz GNSS-gestützter Anwendungen darstellt, ist sie allein nicht ausreichend um eine vollständige Integrität, Vertrauenswürdigkeit und Verfügbarkeit der PNT-Informationen zu gewährleisten. Aufgrund dessen müssen die Detektionsmaßnahmen immer mit technisch und operativ wirksamen Reaktionen kombiniert werden.

5.2.1 Funkbasierte Ortungssysteme und Systemintegration

Funknetzbasierende Systeme, wie Long Range Navigation System (LORAN) und TACTical Air Navigation (TACAN) können bei der Schaffung von robustem GNSS unterstützen. Da diese allerdings ebenfalls störbar sind, dienen sie nicht als alleiniger Unterstützer (MÜLLER 2008). Eine klassische Lösung ist das Vorhalten eines Parallelsystems, auch Back-up-System genannt (BAUER 2014). Hier ist es wichtig, dass dieses zusätzliche System so gut wie störungssicher ist. Ein mögliches System ist das terrestrische Ortungssystem enhanced LORAN (eLORAN). Dabei werden mittels differenzieller Verfahren präzise Zeitinformationen zur Verfügung gestellt (BAUER 2014).

eLORAN ist eine Weiterentwicklung des LORAN und kann im Gegensatz zum Vorgänger, welcher die Hyperbelortung verwendete, mittels Trilateration positionieren. Die Trilateration beschreibt die Positionsbestimmung mittels der Entfernungsmessung zu drei Punkten. Bei der Hyperbelortung werden die hyperbelförmigen Standlinien aus der zeitlichen Differenz der eintreffenden Signale und daraus die Position berechnet. Die genaue Beschreibung kann in BAUER (2014) nachgelesen werden. Ein anderes Parallelsystem ist TACAN. Mithilfe von TACAN erfährt ein Flugzeug, in welcher Richtung und Entfernung es sich in Bezug zu einer Bodenstation befindet (EUROCONTROL 2022). Hierbei werden periodisch gesendete Morsecodes verwendet.

Eine weitere Möglichkeit ist die Integration von GNSS und einem INS (BAUER 2017). Wie bereits im Unterkapitel 3.3.1 erwähnt, werden beim INS Beschleunigungsmesser und Drehratensensoren verwendet. Drehratensensoren erfassen die Rotationsgeschwindigkeit eines Objekts um die zueinander senkrecht stehende Achsen. INS ermöglichen auf Basis dieser Daten, solange der Anfangsort und die Anfangsgeschwindigkeit bekannt sind, eine fortlaufende Positionsbestimmung durch Koppelnavigation unabhängig von elektromagnetischen Signalen. Aufgrund der sich ergänzenden Eigenschaften der beiden Systeme, welche genauer in BAUER (2017) nachgelesen werden können, ist die Kombination sinnvoll.

Es gibt drei Integrationsstufen von INS und GNSS. Bei der lockeren Integration (engl. loose Integration) werden die Navigationslösungen der einzelnen Systeme kombiniert, wobei die Sensoren unabhängig voneinander arbeiten. Außerdem wird das INS durch die GNSS-Daten aktualisiert. Die enge Integration (engl. tight Integration) nutzt die Rohdaten, wie Pseudostrecken und Dopplerverschiebungen, aus dem GNSS gemeinsam mit den INS-Daten. Dadurch sind weniger als vier Satelliten zur Positionierung nötig. Bei der ultra-engen Integration (engl. deep /ultra-tight Integration) werden die GNSS-Lösungen verwendet, um das INS zu kalibrieren. Auch wenn die integrierten GNSS/INS-Empfänger mit zunehmender Integrationsstufe unempfindlicher gegen elektromagnetische Störsignale werden, ist eine vollständige Störtoleranz nicht gewährleistet.

5.2.2 Signalintegration und Antennentechnologie

BAUER (2017) zufolge lassen sich einige GNSS-Störungen mittels Filterung der Signale vermeiden. Hierbei gibt es drei Ausführungen des Filterns. Beim räumlichen Filtern wird die Empfangscharakteristik der Antenne genutzt, um Störquellen gezielt auszublenden. Herkömmliche GNSS-Antennen haben eine reduzierte Empfindlichkeit für Signale in Bodennähe, wodurch sie eine gewisse Grundresistenz gegenüber auf dem Boden stehenden Störsendern aufweisen. Fortgeschrittene Verfahren des räumlichen Filterns nutzen sogenannte Antennengruppen, bei denen mehrere Einzelelemente so kombiniert werden, dass sie gezielt auf bestimmte Richtungen empfindlich reagieren können. Dieses Prinzip ermöglicht die adaptive Steuerung der Empfangscharakteristik, die sogenannte Richtstrahlformung, zur gezielten Unterdrückung von Störsignalen.

Die zweite Art des Filterns (BAUER 2017), das zeitliche Filtern, adressiert vor allem impulsartige Störungen, wie sie beispielsweise durch TACAN und DME entstehen. Ein verbreitetes Verfahren ist das Pulse Blanking, bei dem starke Impulse, die eine festgelegte Amplitudenschwelle überschreiten, ausgeblendet werden. Es besteht das Risiko, dass auch wenn diese Methode einfach umzusetzen ist, relevante GNSS-Signalanteile verloren gehen. Dies geschieht besonders bei häufiger Pulsüberlagerung aus verschiedenen Quellen. BAUER (2017) schlägt vor, um die DME-/TACAN-Interferenz zu bekämpfen, das Puls Blanking mit der dritten Filtermethode dem Frequenzfiltern zu kombinieren.

Das frequenzbasierte Filtern erfolgt typischerweise mit Kerbfiltern, die gezielt enge Frequenzbereiche aus dem Signal unterdrücken (BAUER 2017). Sie eignen sich besonders für schmalbandige oder CW-Störer. Ein Problem dabei ist, dass die Störfrequenz oft nicht konstant oder im Voraus nicht bekannt ist. Ist dies der Fall, dann kommen adaptive Kerbfilter zum Einsatz. Diese analysieren mithilfe von Short-Time-Fourier-Transformation (STFT) die zeitlich wechselnden Frequenzanteile im Signal. Auf dieser Grundlage kann der Filter störende

Frequenzen erkennen und abschwächen, dies geschieht beispielsweise durch das Nullstellen (zeroing) oder das Herabsetzen einzelner Frequenzanteile. Anschließend wird das Signal wieder in den Zeitbereich überführt, wodurch die Verarbeitung der GNSS-Signale mit reduzierter Störbelastung möglich bleibt.

Außerdem kommen spezielle Antennensysteme wie Nulling-Antennen zum Einsatz, die in bestimmte Richtungen eine Empfangsdämpfung erzeugen. Noch leistungsfähiger sind Beamforming-Antennen, deren Richtcharakteristik sich in Echtzeit anpassen lässt. Dies hat den Effekt, dass die Antennengruppe so gesteuert werden kann, dass Störquellen unterdrückt und GNSS-Signale gezielt verstärkt empfangen werden.

JONES (2017) fasst diese Antennengruppen mit Richtcharakteristik unter dem Begriff Controlled reception pattern antenna (CRPA) zusammen. In der Vergangenheit sind diese Antennen ausschließlich in militärischer Nutzung zum Schutz vor Jamming gewesen, dies hat sich mit der Zeit verändert. Künftige CRPA-Systeme werden kompakter, multifunktional und stärker integriert. Dies geschieht in der Kombination von Kommunikations-, Radartechnologien sowie weiteren elektromagnetischen Wellen und es kann in beengten urbanen Umgebungen durch diese Antennensysteme profitiert werden. Diese Antennen sind allerdings aktuell auf GNSS-Verfahren beschränkt, die die Pseudoranges auswerten (BLUM et al. 2023). Bezüglich der Nachrüstung solcher Geräte, die den konventionellen GNSS-Empfängern vorgeschaltet sind, gibt es bereits Systeme, die in der Produktreife sind (HEIL 2024).

Mögliche Kombinationen von räumlich-zeitlichen Filtern und deren Auswirkungen auf Jamming, können aufgrund der Kürze der Arbeit nicht dargestellt werden und sind beispielsweise in TASDEMIR et al. (2014) nachzulesen. Eine Möglichkeit, auf die der Anwender achten kann, ist die Verwendung von Mehrfrequenzempfängern mit integriertem RAIM, da es unwahrscheinlicher ist, dass alle GNSS-Frequenzbänder gestört werden (BAUER 2017). Der militärische Anwender kann zusätzlich beim Kaltstart von GPS-Geräte die verschlüsselte L2-Band nutzen, um eine höhere Resilienz hervorzurufen. Außerdem ist FINK (2013) zufolge wichtig, dass das GNSS-Empfangssystem optimal aufeinander abgestimmt ist, damit die Immunität gegen Jamming und Spoofing verbessert werden kann.

5.2.3 Kryptographische Schutzmaßnahmen und Authentifizierung

Ein wesentliches Element zur Abwehr von GNSS-Störungen ist die Erhöhung der Anti-Jamming-Fähigkeit von GPS-Empfängern (SCHMIDT 2013). Die Abbildung 5-5 verdeutlicht den Zusammenhang zwischen der Entfernung eines Störsenders, dessen Sendeleistung und der erforderlichen Störfestigkeit des GPS-Empfängers in dB, um weiterhin eine zuverlässige Signalverarbeitung zu ermöglichen. Die Störfestigkeit ist durch das J/S-Verhältnis dargestellt. Die schwarzen Linien verdeutlichen die verschiedenen Störsendeleistungen in äquivalenter Strahlungsleistung von 10 mW bis 100 kW. Die roten Linien zeigen die Anti-Jamming-Schwellen verschiedener Betriebsmodi (rechts) von GPS-Empfängern, wobei mit Mspot ein M-Code mit Spot-Beam Unterstützung gemeint ist. Die Abbildung zeigt die unterschiedlichen Empfindlichkeiten der GPS-Modi und welche Unterschiede durch Anti-Jamming-Methoden erreicht werden können. Außerdem wird auch hier nochmal deutlich, welche reale Bedrohung für GNSS-basierte Navigation von leistungsstarken Störern ausgeht.

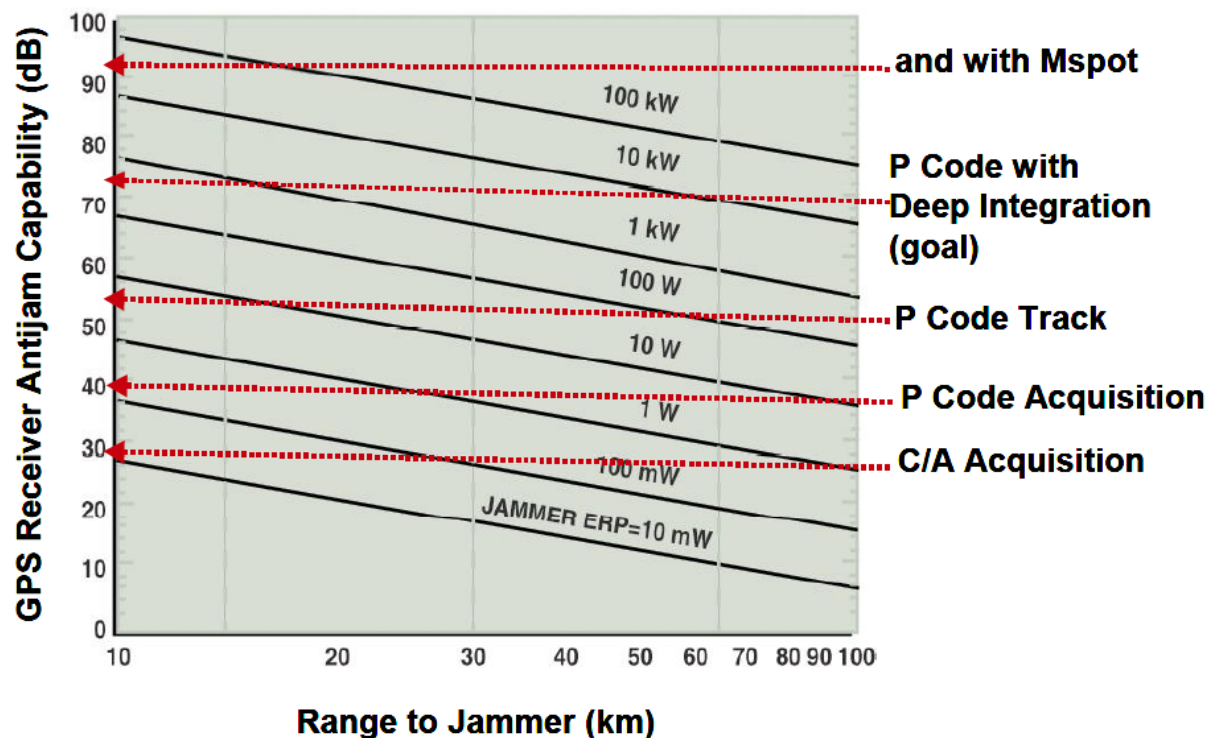


Abb. 5-5: mögliche Anti-Jamming-Fähigkeiten (SCHMIDT 2013)

Die wichtigste anwenderbezogene Methode im Navigation Warfare, welche bereits flächendeckend angewendet wird, ist die Verschlüsselung der Signale beispielsweise mittels GPS-PPS oder der europäischen Entsprechung Galileo-Public Regulated Service (PRS) (SAALBACH 2025). Die Authentifizierung des Signals ist die wohl wichtigste Spoofing-Abwehrmethode (BLUM 2022). Dabei werden kryptographische Techniken eingesetzt um sicherzustellen, dass nur originale Signale verarbeitet werden. Die bekannteste ist, dass Anti-Spoofing von GPS. Dies wurde in Unterkapitel 3.2.2 bereits erklärt. BAUER (2017) verweist darauf, dass diese Technologie für alle GNSS existiert.

Ein Beispiel für die Verwendung von Galileo PRS als robuster und kryptographisch gesicherter Navigationsdienst ist das Projekt HALI-Berlin (aus dem Finnischen „HälytysAjoneuvojen Liikennevaloetuudet“, auf Deutsch „Ampelsteuerung für Einsatzfahrzeuge“), bei dem Spoofing und Jamming-Angriffe auf Einsatzfahrzeuge verhindert werden soll (OERTEL et al. 2022). Im Gegensatz zu offenen GNSS-Signalen bietet PRS eine hohe Störfestigkeit und Authentizität, durch die Ergänzung von INS wird die Positionsbestimmung bei Signalverlust beispielsweise in Tunneln gewährleistet. In diesem Projekt werden zusätzlich die Ampelschaltungen auf die Einsatzfahrzeuge angepasst. HALI-Berlin demonstriert ein resilient aufgebautes System zur zuverlässigen Fahrzeugortung in sicherheitskritischen urbanen Anwendungen. Details können in OERTEL et al. (2022) nachgelesen werden.

Im zivilen Anwendungsbereich werden als Pendant die folgenden beiden Authentifizierungsmethoden entwickelt. Anwender können den Galileo Open Service Navigation Message Authentication (OSNMA) verwenden, um Spoofing zu bekämpfen (GOTTIFREDI et al. 2022). OSNMA ist ein Authentifizierungsmechanismus, der digitale Signaturen in die Navigationsnachricht integriert. Dadurch kann ein GNSS-Empfänger prüfen, ob die empfangenen Navigationsdaten tatsächlich von Galileo stammen und nicht manipuliert oder gefälscht wurden. OSNMA wird beispielsweise in Anti-theft Robust Galileo-based Operational System (ARGOS) genutzt, um Boote vor beispielsweise Diebstahl zu schützen.

Eine Sicherheitsfunktion für das GPS-Signal L1, welches vor Spoofing-Angriffen schützt ist das Chips Message Robust Authentication (CHIMERA) (CAMERON 2019). Dabei werden verschlüsselte Signaturen in das Satellitensignal eingebettet, deren Entschlüsselungscode erst mit Zeitverzögerung gesendet wird. Dadurch kann ein GPS-Empfänger nachträglich Prüfen, ob ein Signal echt oder manipuliert ist.

5.2.4 Operative, strategische und gesellschaftliche Gegenmaßnahmen

Zusätzlich kann als Gegenmaßnahme angesehen werden, dass ein Jammer oder Spoofer zerstört wird. Militärisch beinhaltet dies das kinetische Wirken auf Jammer oder Spoofer zur Zerstörung. Die vorherige Möglichkeit der Detektion und Lokalisierung wurde bereits im vorherigen Unterkapitel beschrieben. WESTBROOK (2019) äußert sich ebenfalls zum Thema Gegenmaßnahmen von Jamming. Er schreibt, dass diese üblicherweise in Systemen und Strukturen integrierten Gegenmaßnahmen erkennen sollen, wann Jamming und Spoofing auftreten. Anschließend die Standorte der Störquellen identifizieren, Alternativsysteme aktivieren oder einfache Störungen ignorieren beziehungsweise überwinden sollen. Zudem sollen die Gegenmaßnahmen gezielt in Metropolregionen oder Regionen mit kritischer Infrastruktur positioniert werden, um größere Schäden zu vermeiden (WESTBROOK 2019). Außerdem kann Anti-Jamming-Software einen Beitrag zur Bekämpfung von Jamming leisten, da diese mit Algorithmen nach Jamming suchen und anschließend dieses unterdrücken kann (FINK 2013). Diese Algorithmen bestehen aus logischen Analysen und Vergleichen verschiedener Signale über höhere Bandbreiten bis hin zu statistischen Auswertungen.

KRIESEWETTER (2024) legt einen etwas anderen Schwerpunkt in der Definition von Gegenmaßnahmen. Neben den erwähnten Multi-GNSS, Multi-Sensoren und Multi-PNZ, soll der Fokus ebenfalls auf Sensibilisierungs- und Bildungsmaßnahmen gelegt werden. Dabei soll die GNSS-Abhängigkeit in kritischer Infrastruktur verringert und die alternativen Methoden der Navigation gestärkt werden. Zudem soll Open Source Intelligence und unabhängige Forschungseinrichtungen, welche zum Thema Identifikation und Analyse von Störungen arbeiten, weiter gestärkt werden, um einen detaillierteren Einblick in das Themenfeld GNSS-Störungen zu liefern. Als Reaktion auf die Herausforderungen der modernen Kriegsführung, wie den Baltic Jammer, nennt er ein koordiniertes Vorgehen auf nationaler und internationaler Ebene als besonders wertvolle Gegenmaßnahme, um die Widerstandsfähigkeit gegen Störungen zu fördern. Als Zusatz zur technischen Weiterentwicklung ist ihm der rechtliche und diplomatische Umgang mit GNSS-Störungen ebenso wichtig.

Abschließend lässt sich festhalten, dass eine Resilienz gegenüber GNSS-Störungen nur durch ganzheitliche Maßnahmenbündel erreicht werden kann. Die genannten Maßnahmen bieten dabei ebenso essenzielle Schutzmaßnahmen wie kryptographische Authentifizierung und hybride Sensorsysteme. Ergänzt werden diese durch operative, organisatorische und strategische Maßnahmen, die sowohl auf Sensorebene als auch im institutionellen Umfeld greifen müssen. Nur durch das Zusammenspiel dieser Ansätze kann die Funktionssicherheit GNSS-basierter Anwendungen in kritischen Bereichen langfristig gewährleistet werden.

5.3 Alternative Navigationsverfahren zum GNSS

Angeichts der Verwundbarkeit und der zunehmenden Abhängigkeit kritischer Infrastrukturen von GNSS stellt sich die Frage, welche Technologien alternativ oder ergänzend eingesetzt werden können, um eine robuste und zuverlässige Positions-, Navigations- und Zeitbestimmung sicherzustellen. Dieses Kapitel beleuchtet und bewertet daher verschiedene GNSS-unabhängige Ansätze. Die jeweilige Bewertung der Alternativen, mittels kurzer Darstellung der Vor- und Nachteile, erfolgt, sofern nicht explizit gekennzeichnet, aufgrund der Einschätzungen der Autorin und unabhängig von Fachliteratur.

5.3.1 Etablierte Verfahren und Systeme

Eine vielversprechende Alternative zur Zeit- und Positionsbestimmung bei GNSS-Ausfall sind hochpräzise interne Zeit- und Taktgeber, wie Kristall- und Rubidium-Oszillatoren (RETERSKI 2015). Diese werden während des GNSS-Betriebs synchronisiert und können danach für Wochen bis Monate stabile Zeitangaben liefern. Das US-Militär nutzt bereits energieeffiziente Chip-Scale-Atomic Clocks (CSACs) und entwickelt Combines State-of-the-art Chip-scale Atomic Navigation (C-SCANs), die Atomuhren mit Inertialsensoren kombinieren (RETERSKI 2015). Dadurch wird eine kontinuierliche Ortung auch ohne GNSS ermöglicht beispielsweise für UAV oder militärische Einsätze unter Störbedingungen. Diese Technologien sind kein vollständiger GNSS-Ersatz, bieten aber eine hohe Resilienz durch Unabhängigkeit von externen Signalen und damit Schutz vor Jamming und Spoofing. Ihre Miniaturisierung erlaubt den Einsatz in mobilen Systemen. Nachteile sind die begrenzte Langzeitgenauigkeit und hohe Kosten. Für militärische und sicherheitskritische Anwendungen stellen sie jedoch eine wertvolle Ergänzung dar.

TACAN stellt wie bereits erwähnt eine bewährte terrestrische Navigationsalternative dar, die im militärischen Luftfahrtbereich ihre Anwendung findet. Als GNSS-Alternative bietet TACAN den Vorteil der Unabhängigkeit von Satellitensignalen und der daraus resultierenden Resistenz gegen Störungen und Ausfällen von GNSS-Systemen. Allerdings sind die Abdeckungen und Genauigkeiten im Gegensatz zu GNSS-basierten Lösungen begrenzt, dadurch wird die Einsatzmöglichkeit eingeschränkt. Die umfangreiche Infrastruktur der Bodenstationen bei TACAN ist wartungsintensiv und kostspielig. Insgesamt kann TACAN als Backup-System oder zur GNSS-Ergänzung dienen, ist jedoch für hochpräzise und flächendeckende Navigation im zivilen Bereich weniger vorgesehen.

Das ebenfalls bereits erklärte DME stellt eine etablierte bodengestützte Navigationshilfe dar, die vor allem in der Luftfahrt verbreitet ist. Sie hat den gleichen Vorteil wie TACAN. Beim DME ist die Reichweite begrenzt und es ist abhängig von den Sichtverbindungen zu Bodenstationen, was die Nutzung in beispielsweise abgelegenen oder schwierig zugänglichen Gebieten

einschränkt. Zudem liefert DME primär Entfernungsinformationen und erfordert die Kombination mit anderen Systemen zur vollständigen Positionsbestimmung. Aufgrund dieser Faktoren kann DME als ergänzende Backup-Lösung zu GNSS oder anderen Systemen dienen, ist jedoch keine alleinige Alternative für hochpräzise globale Navigation.

Auch das bereits erwähnte dynamische Positionieren von Schiffen, meist Offshore, nutzt Ergänzungssysteme parallel zu GNSS aufgrund der Störanfälligkeit von GNSS (OFFSHORE ENGINEERING 2021). Es werden zusätzliche Sensoren verwendet, wie ein Kreiselkompass, Bewegungs-, Wind- und Strömungssensoren und Lasersysteme oder akustische Systeme. Die Verwendung von Ergänzungssystemen bringt die Vorteile der höheren Redundanz und Ausfallsicherheit, aber auch der genaueren Positionsbestimmung mit sich, dies ist gerade bei Offshore-Anlagen unerlässlich. Nachteile wie eine höhere Systemkomplexität und steigende Kosten, sollten ebenfalls beachtet werden. Im Bereich Offshore ist die Nutzung von Ergänzungssystemen indiskutabel aufgrund der fehlenden Störfestigkeit von GNSS und der großen Auswirkungen bei fehlerhaften Positionierungen.

Eine Alternative zum klassischen GNSS-Signal ist der Pseudo Satellit (Pseudolite) (Abb. 5-6), welcher einen bodengestützten Sender darstellt und ein GNSS-ähnliches Signal ausstrahlt (MEURER 2024). Sie können als zusätzliche Signalquelle, wie ein GNSS-Satellit genutzt werden. Pseudolites verwenden spezielle PRN-Codes und eine abweichende

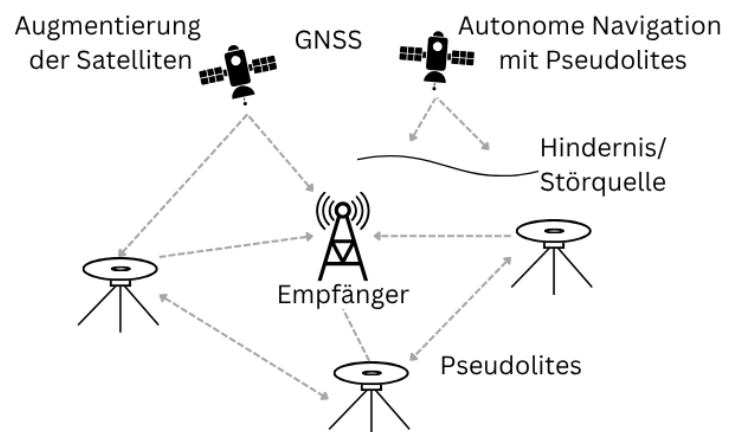


Abb. 5-6: Pseudolite (geändert nach MEURER 2024)

Navigationsmessage, die anstatt den Ephemeriden die Koordinaten des Pseudolites und Zusatzinformationen enthält. Die genauen Frequenzbereiche können in MEURER 2024 nachgelesen werden. Zusätzlich zur Verbesserung der Integrität und Genauigkeit wird dadurch die Geometrie verbessert. Es werden keine zusätzlichen Antennen oder Empfänger benötigt, die GNSS-fähigen Materialien genügen. Pseudolites stellen zusätzlich eine Gegenmaßnahme beim Jamming dar, durch höhere Sendeleistung und robustere Signale (MEURER 2024). Nachteile die MEURER (2024) nennt sind stärkere Mehrwegeausbreitungen durch einen flachen Einfallswinkel der Signale, ein schlechtes Rausch-/Entfernungsverhältnis und die Zeitsynchronisation von Pseudolites zu GNSS-Zeit, welche schwierig zu realisieren ist. Die aktuellen Anwendungsbereiche, die MEURER (2024) nennt, zeigen, dass dies eine sinnvolle Alternative und gegebenenfalls Ergänzung zu GNSS darstellt, allerdings aufgrund der Nachteile auch nicht in jedem Bereich.

Seamless Navigation ist nach PELTORA et al. (2017) definiert als nahtlose Navigation. Dies bedeutet, dass mithilfe eines optimal konzipierten Navigationssystem, welches diverse verfügbare Positionierungstechnologien, wie GNSS, Funktechnologien und akustische Verfahren vereint, eine großflächige Abdeckung aller möglichen Szenarien und Umgebungen lückenlos sichergestellt werden kann (PELTORA et al. 2017). Diese lückenlose Abdeckung ist ein großer Vorteil den Seamless Navigation mit sich bringt, ebenso wie die Kombination vieler Technologien und deren Vorteile. Ein Nachteil könnte die hohe Dichte an Technologien sein, wodurch ein technischer Teil- oder Gesamtausfall wahrscheinlicher wird. Es stellt definitiv eine gut umsetzbare und flächendeckend einsetzbares hybrides Systemkonzept dar.

Die wohl relevanteste Alternative zu GNSS, welche ebenfalls auch im Bereich Seamless Navigation eingesetzt wird, ist das inertiale Navigationssystem, sei es als Kombination mit GNSS oder als eigenständige Technologie. Aufgrund dieser Technologie erhöht sich die Jamming-Resistenz und durch die kompakte Bauweise eignet es sich gerade für militärische Zwecke und Anwendungen mit extremen dynamischen und elektromagnetischen Anforderungen (SCHMIDT 2013). Wird INS allerdings ohne GNSS eingesetzt, wird es auf Dauer ungenau und die Position, bei der es sich ohnehin lediglich um eine relative Position handelt, wird fehlerhaft (PELTORA et al. 2017). Nichtsdestotrotz ist es robust gegen Störungen und ein unverzichtbarer Teil hybrider Navigationssystem und kann eine sehr gutes Ergänzungssystem zu GNSS sein. Die eigenständige Nutzung ist aufgrund der fehlenden Genauigkeit nicht empfehlenswert.

Optische Sensoren stellen eine zusätzliche Navigationskomponente beispielsweise in der Seamless Navigation dar (MEURER 2024). Dabei wird die absolute und relative Position mittels Bilddaten bestimmt. Eine Systemkalibrierung zwischen GNSS/INS und Kamera ist zusätzlich möglich. Die Nutzung dieser visuellen Odometrie⁸ ermöglicht neben der Detektion und Umgehung von GNSS-Spoofing auch die Überbrückung bei GNSS-Ausfall durch beispielsweise Jamming (MEURER 2024). Es birgt den Vorteil der Verbesserung der Genauigkeiten durch die optische Komponente, außerdem können diese nicht gejammt werden. Der größte Nachteil ist die zur Verfügungstellung von Bildmaterialien und die Anfälligkeit für visuelle Veränderungen bei der Positionsbestimmung. Insgesamt ist die Effektivität und die Qualität von der Nutzungsart der Alternative abhängig. Eine Nutzung beispielsweise im Bereich UAV ist als gewinnbringend zu betrachten.

⁸ Methode zur Weg- und Positionsbestimmung durch Messung von Bewegungsdaten, z.B. über Raddrehungen (ROBOT MAKERS 2021)

5.3.2 Technologiekonzepte im Entwicklungsstadium

Um die Nachteile des INS zu umgehen, wird an Quanten-Inertialnavigationssystemen (QINS) geforscht (SCHLIPPERT 2019). Diese weisen deutlich geringere Positionsfehler als herkömmliche INS auf und sind rund 50x genauer (Abb. 5-7) (FUTUREZONE 2025). Ihr Einsatz soll beispielsweise im autonomen Fahren, bei Rettungshubschraubern oder in der Tiefenraumfahrt sein (SCHLIPPERT 2019). Hierbei sollen geführte Materiewelleninterferometer verwendet werden, da sie weniger anfällig für Signalverluste sind. Es sind robuste Messverfahren untersucht worden, um einen kompakten, chipbasierten Sensor für den kommerziellen Gebrauch zu entwickeln (FUTUREZONE 2025). Dieses System befindet sich noch nicht in der Praxis, stellt allerdings aufgrund der Vorteile die ein INS mit sich bringt und der zusätzlichen Positionsgenauigkeit eine sinnvolle zukünftige Alternative dar.

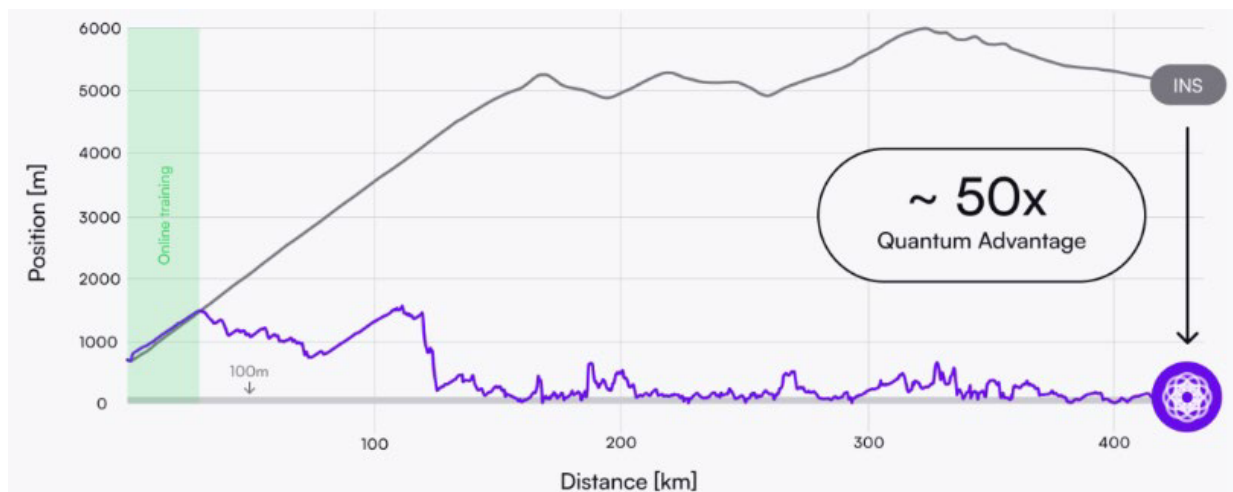


Abb. 5-7: Quanten-INS im Vergleich zu herkömmlichen INS (FUTUREZONE 2025)

Ein experimenteller Ansatz zur GNSS-unabhängigen Navigation basiert auf der Nutzung des Magnetfeldes (SCHWEBER 2020). Das Konzept wird unter dem Namen MAGNAV entwickelt und nutzt hochpräzise Magnetometer zur Erfassung kleiner Anomalien im Erdmagnetfeld. Die Positionsbestimmung soll dadurch in Verbindung mit detaillierten Magnetfeldkarten und modernen Verfahren wie maschinellem Lernen möglich sein. Die Genauigkeit lässt allerdings zu wünschen übrig und liegt bei ungefähr einem Kilometer. Sie hängt außerdem stark von den vorliegenden Karten ab. Ein Vorteil ist die globale Verfügbarkeit, sowie die Wetterunabhängigkeit und das es nicht manipuliert werden kann (SCHWEBER 2020). Besonders relevant ist dieser Ansatz für militärische oder sicherheitskritische Anwendungen, bei denen es hauptsächlich um die Verfügbarkeit und Störresistenz geht, anstatt um zentimetergenaue Positionen (SCHWEBER 2020). MAGNAV bietet ein spannendes, physikalisches Backup-System zu GNSS, insbesondere in Jamming-sensiblen Umgebungen ist es gut vorstellbar. Die Technologie ist aktuell allerdings noch weit von einer praxisreifen Nutzung entfernt. Die geringe Genauigkeit und der enorme Rechen- und Kalibrierungsaufwand stellen noch

ein großes Problem dar. Dennoch ist das Konzept bemerkenswert, da es auf einer natürlichen Referenz basiert und sich zu einem robusten System entwickeln könnte.

Ein anderes Beispiel für die Kombination eines sich in der Entwicklung befindenden Ergänzungssystems mit GNSS, ist die Kombination mit WiFi-Distanzmessung (EUSPA 2021). Hierbei handelt es sich um das Projekt „BANSHEE“ (Abb. 5-8) zur Seamless Navigation zwischen Indoor und Outdoor. Die Nutzung von WiFi als Ergänzung birgt sowohl Vor- als auch Nachteile, da WiFi nicht flächendeckend ohne Verschlüsselung zugänglich ist. Wenn es hingegen verfügbar ist, kann mithilfe der Technologie eine gute Indoor-Navigation geschaffen werden. Bei diesem Ergänzungssystem ist es wie mit jedem Ergänzungssystem, es ist so lange gut und eine Bereicherung, wie man seine Vorteile nutzen kann. Sollten allerdings die Nachteile in den Vordergrund rutschen, bringt es eher neue Herausforderungen als Lösungen.

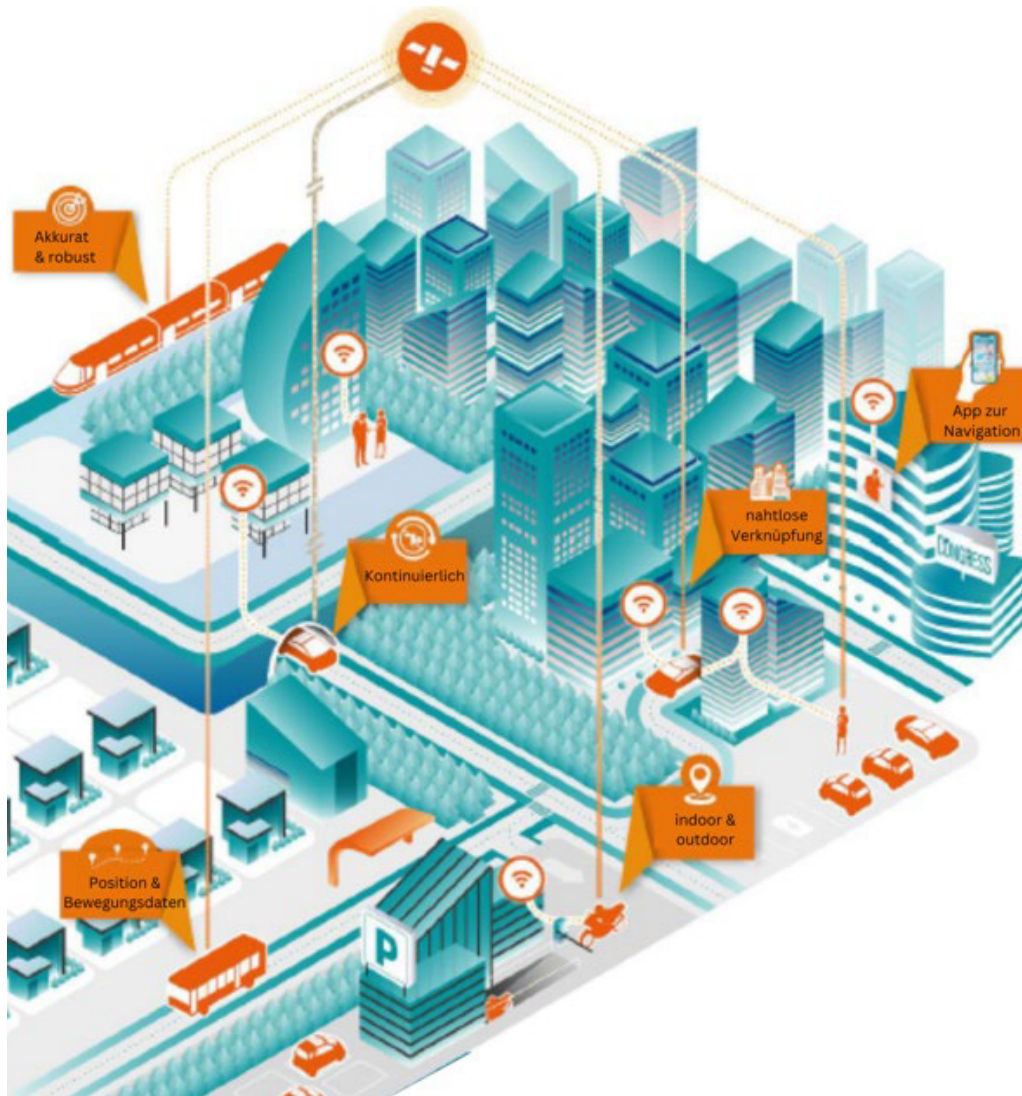


Abb. 5-8: BANSHEE (geändert nach VAL 2022)

Ein innovativer Ansatz zur GNSS-unabhängigen Positions- und Zeitbestimmung sieht die Nutzung bestehender terrestrischer TV-Sendeinfrastruktur vor (ROHDE&SCHWARZ 2023). Durch die Wiederverwendung vorhandener Sendetürme, Verstärker, Frequenzen und Antennen kann mit typischer Sendeleistung von 10 bis 100 kW ein großflächiger Navigationsdienst aufgebaut werden. Dieser Ansatz wird durch die Nutzung des 5G-Broadcast-Standards ergänzt. Dieser stellt UTC-Zeitstempel und Positionsinformationen zur Verfügung. Der Navigationsdienst beansprucht nur minimale Ressourcen und die Hauptfunktion der TV-Übertragung bleibt bestehen. Es sind nur minimale Updates an den bestehenden TV-Sendern nötig (ROHDE&SCHWARZ 2023). Der Vorteil liegt in der kosteneffizienten Nutzung der vorhandenen Infrastruktur und der einfachen Integration in zukünftige Massenmarktgeräte. Auch bei GNSS-Ausfällen können so robuste PNT-Dienste in urbanen Räumen zur Verfügung gestellt werden. Die Abdeckung und Signalstärke bringen eine gute Indoor-Tauglichkeit. Allerdings sind die Genauigkeit und Integrität noch nicht vollständig untersucht. Der weltweite Rollout hängt stark von der Standardisierung und Regulierung ab. Dennoch zeigt dieser Ansatz viel Potential als resiliente Ergänzung oder Backup-System zu GNSS.

Ebenso vielversprechend ist der Ansatz eines Terrestrial Networks (KOELEMEIJ et al. 2022). Es handelt sich um ein terrestrisches Positionierungssystem, dass auf einem Netzwerk aus Funksendern besteht. Diese werden über Glasfaser mit Subnanosekunden-Genauigkeit synchronisiert. Durch den Einsatz spektral effizienter Breitbandsignale und moderner Signalverarbeitung kann das System selbst in urbanen Mehrweg-Umgebungen robuste dezimetergenaue Positionsbestimmung und präzise Zeitverteilung ermöglichen (KOELEMEIJ et al. 2022). Der größte Vorteil dieses Netzwerks liegt in der hohen Genauigkeit trotz schwieriger Umgebungsbedingungen. Zudem könnte bestehende Telekommunikationsinfrastruktur als Grundlage genutzt werden. Derzeit ist es noch im Forschungsstadium und es ist auf den Ausbau der Glasfaserinfrastruktur angewiesen. Langfristig hat es jedoch Potential eine robuste Alternative vor allem in kritischen Anwendungsbereichen zu werden.

LEO-PNT ist ein genauso wie GNSS satellitenbasierter Ansatz zur Navigation (KUNZI 2023). Es wird zum aktuellen Zeitpunkt als Ergänzung oder Alternative zu GNSS erforscht. Durch die deutlich niedrigere Bahnhöhe senden LEO-Satelliten deutlich stärkere Signale aus, was Vorteile in schwierigen Empfangsumgebungen wie Innenräumen oder urbanen Gebieten birgt. Gleichzeitig wird dadurch die Störresistenz gegenüber Jamming und Spoofing erhöht. Für eine weltweite Abdeckung werden jedoch hunderte Satelliten notwendig, da die Ausleuchtungszone einzelner LEO-Satelliten klein sind (KUNZI 2023). LEO-PNT steht eine vielversprechende Perspektive als Alternativ oder Ergänzungssystem dar.

Mode-N ist ein neues terrestrisches Navigationskonzept, das KLEIN (2022) zufolge die veralteten Systeme DME und TACAN ersetzen soll. Es nutzt moderne digitale Signalverarbeitung und basiert auf der Verwendung bestehender DME-Infrastruktur. Es erweitert jedoch deren Funktionalität erheblich. Ziel ist es, eine bodengebundene Navigationslösung bereitzustellen, die hinsichtlich Genauigkeit, Integrität und Verfügbarkeit mit GNSS vergleichbar ist. Dabei jedoch ohne die Verwundbarkeit von GNSS gegenüber Jamming und Spoofing aufgebaut wird (KLEIN 2022). In Abbildung 5-9 ist der geschätzte Positionsfehler in Metern für Flugzeuge innerhalb eines Abdeckungsradius von 100 Seemeilen unter Verwendung vorhandener Überwachungsstandorte als Installationsstandorte für Bodenstationen des Mode N zu sehen (LANGLEY et al. 2021). Als GNSS-Alternative überzeugt Mode-N durch seine hohe Widerstandsfähigkeit gegenüber externen Störeinflüssen und die Nutzung bereits vorhandener Infrastruktur. Allerdings befindet es sich noch in der Entwicklungsphase und erfordert internationale Abstimmung sowie Investitionen in neue Hardware. Daher ist es nicht sofort einsatzfähig. Dennoch bietet Mode-N langfristig ein hohes Potential als resiliente und moderne Ergänzung oder als alternative zu satellitenbasierter Navigation, insbesondere in sicherheitskritischen Anwendungen.

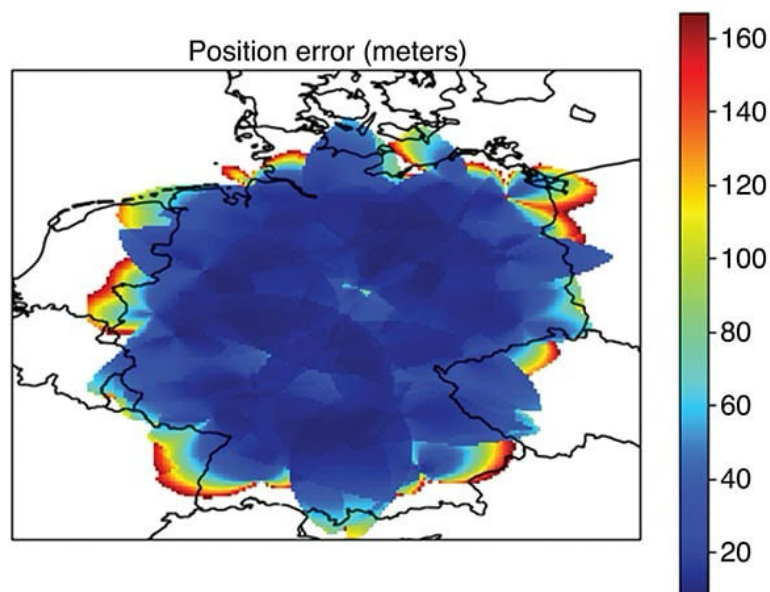


Abb. 5-9: Genauigkeit Mode-N (LANGLEY et al. 2021)

L-band Digital Aeronautical Communications System (LDACS) ist ein zukünftiger Standard im digitalen Flugfunk und soll den bisherigen analogen Sprechfunk im Luftverkehr ablösen (HEIL 2024). Im Rahmen eines europäischen Programms wird LDACS um eine Navigationskomponente namens LDACS-NAV erweitert. Diese Navigationskomponente nutzt die Funksignale des Systems zur Positionsbestimmung und wurde bereits erfolgreich in Flugversuchen, etwa mit dem Forschungsflugzeug Falcon des deutschen Zentrums für Luft- und Raumfahrt (DLR), erprobt (HEIL 2024). LDACS ist primär ein Kommunikationssystem, entwickelt sich mit LDACS-Nav allerdings zu einer vielversprechenden Ergänzung und Backup-

Lösung für GNSS. Als globale, satellitenunabhängige Alternative ist es aufgrund der bodengebundenen Infrastruktur nicht geeignet. Es kann aber in sicherheitskritischen Anwendungen die Resilienz der Luftnavigation erhöhen.

Ein vielversprechender Ansatz im maritimen Bereich ist das Ranging Mode Verfahren (R-Mode). Laut HOPPE (2017) nutzt R-Mode bestehende Infrastrukturen wie Mittelwellen-DGNSS-Sender und das AIS, um präzise Zeitinformationen für die Positionsbestimmung zur Verfügung zu stellen. Ein solcher Sender ist in Abbildung 5-10 zu sehen. Anders als bei DGNSS ermöglicht R-Mode eine vollständige Positionsbestimmung ohne GNSS-Verbindung. Es ist eine subzentimetergenaue Positionierung möglich (HOPPE 2017). GEWIES et al. (2024) zufolge gibt es eine starke Initiative zur Förderung dieses Ansatzes in der Ostsee. Das dazugehörige Projekt nennt sich Operational R-Mode Baltic Sea System to support resilient navigation (ORMOBASS). R-Mode birgt einige Vorteile. Die



Abb. 5-10: R-Mode Sender

(LUFTFAHRTMAGAZIN 2025)

Nutzung von bereits vorhandener Infrastruktur reduziert Kosten und vereinfacht die Inbetriebnahme. Durch eine breitere Nutzung des elektromagnetischen Spektrums würde ein Störer ebenfalls mehr Energie benötigen, um alle Signale zu stören. Dies ist ein weiterer Vorteil von R-Mode. Die Möglichkeit der Kombination diverser Signale wie AIS, Mittelwellen-DGNSS und eLORAN bietet eine Verbesserung der Genauigkeit und Verfügbarkeit. Aktuell liegt die Genauigkeit bei 10 m bis 100 m (GEWIES et al. 2024). Kritisch zu betrachten ist jedoch, dass die Signalabdeckung derzeit auf Küstenregionen beschränkt ist und die Genauigkeit durch beispielsweise Interferenzen und Mehrwegeausbreitung beeinflusst werden kann (HOPPE 2017). Zudem befindet sich dieses System noch in der Testphase und eine flächendeckende Nutzung ist noch nicht realisierbar. Insgesamt lässt sich festhalten, dass R-Mode eine realistische Möglichkeit für ein robustes, terrestrisches Backup-System zur maritimen Navigation ist und bei GNSS-Störungen und Ausfällen hohe Relevanz gewinnen könnte. Für eine konkrete Bewertung ist allerdings die weitere Technologieentwicklung abzuwarten. Die Stärke der Initiative um ORMOBASS, könnte man auf den Baltic Jammer (vgl. 4.4.3) zurückführen.

eLORAN ist nicht nur in Kombination mit R-Mode oder als Backup-System für GNSS von Bedeutung, sondern kann auch als eigenständiges terrestrisches Funknavigationssystem zur Positionsbestimmung genutzt werden. Es basiert auf Langwellensignalen, die gegen Störungen wie Jamming und Spoofing robust sind. Dementsprechend ist es eine verlässliche Alternative zur satellitengestützten Navigation. Trotz seiner Widerstandsfähigkeit ist die Genauigkeit von eLORAN im Vergleich zu GNSS begrenzt und seine Abdeckung ist von der Verfügbarkeit der Senderinfrastruktur abhängig. Es empfiehlt sich die Kombination aus eLORAN mit anderen Systemen, um eine möglichst hohe Verfügbarkeit und Präzision der Positionsdaten zu erhalten. eLORAN befindet sich zwar bereits in der Nutzung, ist allerdings noch nicht vollständig erforscht und entwickelt.

Das auf einem Multi-Layer Perceptron (MLP) basierende Ultra-WideBand (UWB)-Inertiale Messdaten (engl. Inertial Measurement Unit, IMU)-Positionierungssystem stellt eine innovative Möglichkeit dar, insbesondere in anspruchsvollen Umgebungen und GNSS-gestörten Bereichen präzise Lokalisation zu ermöglichen (BAO et al. 2025). Durch die Kombination von UWB-Signalverarbeitung und IMU und deren Fusion mittels einer MLP werden

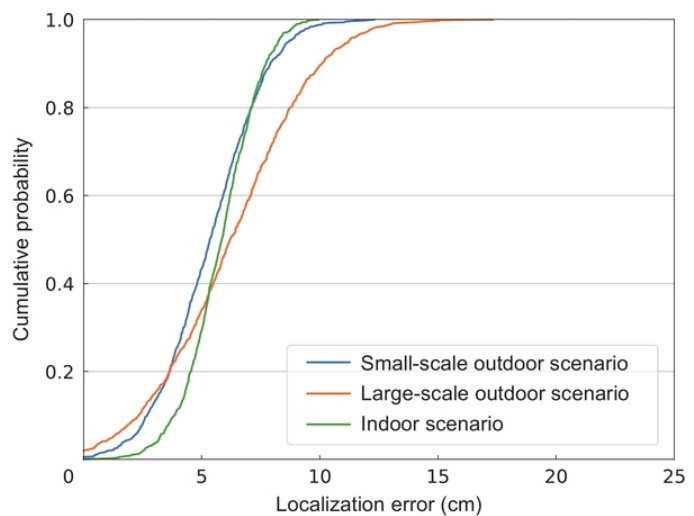


Abb. 5-11: Positionsgenauigkeiten von UAV (BAO et al. 2025)

Messfehler kalibriert und Bewegungsdynamiken des Objektes berücksichtigt (BAO et al. 2025). In BAO et al. (2025) wird diese Technik in UAVs untersucht. Dies zeigt auch die Abbildung 5-11, wobei die X-Achse die Positionsfehler in Zentimetern anzeigt und die Y-Achse die kumulative Wahrscheinlichkeit, also wie groß der Anteil der Messungen ist, die einen Fehler kleiner oder gleich einem bestimmten Wert auf der X-Achse haben. Trotz ihrer hohen Genauigkeit und Flexibilität eignet sich MLP-basierte UWB-IMU-Positionierung jedoch vorwiegend für lokale oder spezifische Anwendungen und kann GNSS nicht flächendeckend ersetzen. Durch die begrenzte Reichweite von UWB ist der Einsatz flächenmäßig begrenzt. Trotz dessen stellt sie eine robuste Ergänzung in urbanen Umgebungen und Anwendungen wie Indoor-Navigation dar. Daher lässt sie sich eher als komplementäre als eine konkurrenzfähige Alternative zu GNSS einstufen.

5.3.3 Resiliente Navigationsverfahren für Not- und Krisenszenarien

Eine sehr alte Form ist die astronomische Ortsbestimmung. Sie wird definiert als die Bestimmung geographischer Koordinaten von Punkten auf der Erdoberfläche anhand von astronomischen Messungen (SPEKTRUM 2000). Dabei ergeben sich die astronomische Breite und Länge. Sie unterscheiden sich von den geodätischen Koordinaten, da ihre Bezugsfläche das Geoid ist und kein mathematisches Ellipsoid. Neben den Koordinaten zählt auch das astrologische Azimut eines Gestirns oder einer terrestrischen Richtung zu den Elementen der Ortsbestimmung. Die genauen Abläufe dieser können in SEPKTRUM (2000) nachgelesen werden.

Angesichts der Verwundbarkeit moderner Navigationssysteme durch Jamming, Spoofing oder Ausfälle wird SAALBACH (2025) zufolge diese Methode seit einigen Jahren wieder vermehrt benötigt, häufig als Notfallsystem. So führte die US-Navy im Jahr 2016 die Ausbildung der Himmelsnavigation mit dem Sextanten (Abb. 5-12) wieder verpflichtend ein, um eine unabhängige Notfallnavigation zu gewährleisten. Auch die britische Royal Navy schreibt vor, dass ihre Schiffe stets einen aktuellen nautischen Almanach für die „emergency celestial navigation“ mitführen müssen (SAALBACH 2025). Die astronomische Ortsbestimmung ist zwar in der Anwendung und Ausbildung aufwändig und wetterabhängig, birgt jedoch den großen Vorteil vollständiger Unabhängigkeit von Technik und Funkverbindungen. Ihre Genauigkeit reicht unter optimalen Bedingungen bis auf wenige hundert Meter (SAALBACH 2025), was sie in vielen zivilen und militärischen Notfallszenarien zu einem robusten Backup macht. Sie ist immun gegenüber elektromagnetischer Störung und stellt damit eine strategisch wertvolle Redundanz zu GNSS-Systemen dar. In Zeiten zunehmender Bedrohungen im Bereich NAVWAR zeigt sich ihre Relevanz nicht nur aus historischer, sondern auch aus sicherheitspolitischer Perspektive.



Abb. 5-12: Sextant (RÖNNBERG 2020)

Vor der Einführung elektronischer Satellitennavigationssysteme bildeten Kompassnavigation und klassische Karten die Grundlage der Positionsbestimmung. Der Magnetkompass ermöglicht anhand des Magnetfeldes die Himmelsrichtungen zu bestimmen (EISENHUT 2025). In Kombination mit Karten (Abb. 5-13) lässt sich so eine grobe bis mäßig präzise Ortsbestimmung durchführen (LICKTEIG 2023). Besonders in der terrestrischen Navigation, im Outdoor-Bereich oder bei



Abb. 5-13: Karte und Kompass (LICKTEIG 2023)

militärischen Einsätzen ohne elektronische Hilfsmittel findet diese Methode bis heute Anwendung. Bei dieser Form der Navigation werden bekannte Punkte, wie geografische Landmarken, Höhenpunkte oder trigonometrische Vermessungspunkte, auf einer Karte lokalisiert und durch Peilungen wie Marschkompasskurse zueinander in Beziehung gesetzt. Mit Methoden wie dem Kreuzpeilungsverfahren oder der Rückwärtsschnittmethode lässt sich der eigene Standort bestimmen (LICKTEIG 2023). Kompass und Vermessungskarten sind als grundlegende robuste Notfalllösung in bestimmten Bereichen sinnvoll, können aber GNSS in modernen, hochdynamischen oder hochpräzisen Anwendungen nicht ersetzen. Ihre Stärke liegt eher in der Ausfallsicherheit und Einfachheit als in der Präzision und Effizienz.

Die zunehmenden GNSS-Störungen machen deutlich wie essenziell eine robuste und resiliente Ausgestaltung von PNT-Systemen gerade für kritische Infrastruktur und sicherheitsrelevante Anwendungen ist. Die in diesem Kapitel beleuchteten Technologien geben einen Überblick über die verschiedensten alternativen Verfahren, von hochmodernen Konzepten bis hin zu altbewährten klassischen Verfahren.

6 Zusammenfassung

Die präzise Bestimmung des eigenen Standortes ist eine fundamentale Voraussetzung für zahlreiche zivile und militärische Anwendungen. Ziel dieser Arbeit war es, die Verwundbarkeit von GNSS gegenüber gezielten Störungen wie Jamming und Spoofing systematisch zu untersuchen, deren Auswirkungen in unterschiedlichen Anwendungsbereichen aufzuzeigen und potenzielle Gegenmaßnahmen zur Steigerung der Robustheit von GNSS zu analysieren. Das zitierte Statement „Wenn Sie nicht wissen, wo Sie sind, sind Sie eigentlich tot!“ verdeutlicht die existenzielle Bedeutung von zuverlässiger Navigation, insbesondere in Einsatzszenarien. Mit der Entstehung globaler Navigationssatellitensysteme hat sich die PNT-Bestimmung grundlegend revolutioniert. Gleichzeitig birgt die starke Abhängigkeit von einer einzelnen Technologie erhebliche Risiken.

Im Verlauf der Arbeit wurden die technischen Grundlagen, Funktionsweisen sowie zivil-militärische Einsatzszenarien von GNSS-Störungen umfassend dargestellt. Fallbeispiele aus aktuellen Konfliktregionen wie dem Russland-Ukraine Krieg sowie weitere sicherheitspolitische Aspekte verdeutlichen die Brisanz und Aktualität des Themas. So zeigt sich etwa, dass GNSS-Störungen bereits zu signifikanten Beeinträchtigungen in der zivilen Luftfahrt, militärischen Drohneneinsätzen und maritimen Logistik geführt haben. Eine sektorübergreifende Analyse offenbarte dabei unterschiedliche Verwundbarkeiten, insbesondere bei kritischen Infrastrukturen, die auf präzise Positions-, Navigations- und Zeitinformationen angewiesen sind. Es werden spezifische Herausforderungen und Gefährdungspotenziale in den einzelnen Sektoren herausgearbeitet, um ein ganzheitliches Verständnis der Problematik zu ermöglichen. Insbesondere wird deutlich, dass gerade kritische Infrastrukturen und sicherheitsrelevante Operationen durch GNSS-Ausfälle erheblich gefährdet sind. Es werden die Auswirkungen von GNSS-Störungen auf unterschiedliche Anwendungsbereiche der Navigation, darunter maritime, luft- und bodengestützte Systeme, analysiert. Beispielhafte Vorfälle wie AIS-Manipulation in der Schifffahrt, GPS-basierte Betrugsversuche im Straßenverkehr oder gezieltes militärisches Jamming unterstreichen die sektorübergreifende Bedrohungslage und die Bandbreite der betroffenen Systeme.

Ein zentraler Bestandteil der Arbeit ist die Untersuchung und Bewertung von Detektionsmethoden und ergänzenden Navigationsverfahren zur Erhöhung der Resilienz gegen Jamming und Spoofing. Von klassischen Methoden wie der Sternnavigation über inertielle und quanteninertielle Systeme bis hin zu modernen Ansätzen wie LEO-Satelliten, optische Sensorik und terrestrischen Netzwerken wurde ein breites Spektrum analysiert. Besonders vielversprechend ist die Kombination dieser Technologien im Sinne eines „Seamless Navigation“-Ansatzes. Hybride Systeme, die GNSS etwa mit INS, optischer Navigation und terrestrischen Signalen koppeln, erhöhen nicht nur die Ausfallsicherheit, sondern liefern auch

robustere und präzisere Positionsdaten. Die Analyse zeigt deutlich, dass keine einzelne Technologie GNSS vollständig ersetzen kann. Entscheidend ist ein intelligentes Zusammenspiel mehrerer Verfahren, angepasst an den jeweiligen Anwendungsfall. Gerade in politisch instabilen Zeiten, die von Jamming und Spoofing als Machtinstrument geprägt sind, sollten ebenfalls resiliente Notfallsysteme nicht außer Acht gelassen werden und insbesondere im militärischen Kontext weiterhin genutzt werden. Neben technologischen Maßnahmen ist auch der Aufbau realitätsnaher Übungsszenarien entscheidend, um Systeme und Personal auf Navigationsausfälle vorzubereiten.

Abschließend zeigt die Arbeit, dass trotz vielfältiger Alternativen und technologischer Fortschritte keine einzelne Lösung GNSS vollständig ersetzen kann. Vielmehr liegt die Zukunft in einem intelligenten Zusammenspiel verschiedener Systeme, um Ausfallsicherheit und Integrität der PNT-Informationen zu gewährleisten. Nur so kann den wachsenden Bedrohungen durch Störungen und Manipulation wirksam begegnet und die Sicherheit kritischer Infrastrukturen sowie militärischer Anwendungen gewährleistet werden. Jede Technologie besitzt Stärken und Schwächen, allerdings kann keine dieser Lösungen GNSS vollständig ersetzen. Die Zukunft sollte daher nicht auf der Suche nach der einen Alternative liegen, sondern auf einem intelligenten Zusammenspiel verschiedener Technologien zur Sicherstellung einer störresistenten PNT-Versorgung.

Der eingangs zitierte Ausspruch erhält somit eine vertiefte Bedeutung: Nicht nur die Kenntnis des aktuellen Standortes, sondern auch die Gewissheit über dessen Verlässlichkeit und die Fähigkeit, sich auch bei Störungen sicher zu orientieren, sind heute essenziell. In einer Zeit zunehmender Komplexität und Gefährdung der Navigationssysteme wird die Entwicklung resilienter PNT-Technologien zur Schlüsselaufgabe in vielen sicherheitsrelevanten Bereichen. Bei der Entwicklung dieser Technologien sollte der Kosten-Nutzen-Faktor beispielsweise von Ausbau- und Instandhaltungsaufwand mit einbezogen werden.

Für die Zukunft zeigt sich, dass die Integration neuer Technologien zur Störungsdetektion großes Potential mitbringen, die Robustheit von Navigationssystemen weiter zu steigern. Zudem sind internationale Kooperationen zur Standardisierung und Absicherung der Navigationsinfrastruktur unabdingbar, um auf globale Bedrohungen durch Störungen reagieren zu können. Die Weiterentwicklung von terrestrischen Netzwerken und Satellitenkonstellationen im LEO könnte zudem die Abhängigkeit von klassischen GNSS reduzieren. Schließlich wird der Ausbau eines ganzheitlich, nahtlos funktionierenden, sensorübergreifenden Gesamtsystems entscheidend sein, um in allen Umgebungen und Einsatzszenarien zuverlässige PNT-Daten sicherzustellen. Die gezielte Kombination der Verfahren ist sinnvoll, zum Nachteilsausgleich und sie auf den jeweiligen Anwendungsfall zuzuschneiden. Dies ist sowohl aus technischer als auch aus geopolitischer Perspektive eine zentrale Herausforderung der kommenden Jahre.

Diese Arbeit bietet eine breite und interdisziplinäre Übersicht, erhebt jedoch keinen Anspruch auf vollständige Tiefe. Einzelne Technologien konnten lediglich ansatzweise diskutiert werden, da deren praktische Anwendung noch Gegenstand aktueller Forschung ist und es den Umfang dieser Arbeit übersteigen würde. Zudem beschränkt sich die Betrachtung auf öffentlich zugängliche Informationen und geheimdienstliche oder militärisch klassifizierte Systeme konnten nicht berücksichtigt werden.

Die zentrale Frage dieser Arbeit lautete, wie PNT-Informationen auch unter gezielter Störung durch Jamming und Spoofing zuverlässig bereitgestellt werden könnte. Die Antwort liegt in einem systematischen, technologieoffenen Ansatz, der Redundanz, Vielfalt und Anpassungsfähigkeit in den Mittelpunkt stellt. Der allerdings altbewährte und zeitlose Möglichkeiten als Notfalloptionen nicht unberücksichtigt lässt.

7 Literaturverzeichnis

- BAO, BINBIN; LUO, CHUANWEN; HONG, YI; CHEN, ZHIBO & XIN FAN (2025): High-Precision UAV Positioning Method Based on MLP Integrating UWB and IMU. – Online in Internet: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10817766> [Stand: 2025-06-27].
- BAUER, MANFRED (2014): eLORAN – Renaissance eines Ortungsverfahrens. – In: Hydrographische Nachrichten, Ausgabe 98, S. 26-30. – Und Online in Internet: https://www.dhyg.de/images/hn_ausgaben/HN098.pdf [Stand: 2025-06-24].
- BAUER, MANFRED (2017): Vermessung und Ortung mit Satelliten: Globale Navigations-satellitensysteme (GNSS) und andere satellitengestützte Navigationssysteme, 7. Auflage, Berlin – Und Online in Internet: <https://content-select.com/de/portal/media/view/5a8a9ac2-ffc0-481f-b518-1a13b0dd2d03?forceauth=1> [Stand: 2025-05-13].
- BERGMANN, BJORN & KELLY FRANKLIN (2023): Tankers Falsify AIS Tracking Positions to Hide Entry into Russian Black Sea Ports. – Online in Internet: <https://skytruth.org/2023/05/tankers-falsify-ais-tracking-positions-to-hide-entry-into-russian-black-sea-ports/> [Stand: 2025-06-12].
- BLUM, RICHARD (2022): Interferenz von GNSS-Signalen. – Unveröffentlichte Masterarbeit an der Hochschule Bochum.
- BLUM, RICHARD; GÖRRES, BARBARA & BRIGITTE GUNDLICH (2023): Störung des GNSS – eine reale Gefahr! – In: GNSS 2023 – Zeit für ein Update?! – Beiträge zum 219. Seminar der INTERGEO akademie am 4. und 5. September 2023 in Bochum. – Und Online in Internet: https://geodaesie.info/images/schriftenreihe/downloads/DVW_106_2023_GNSS_2023_FINAL_230816.pdf [Stand: 2025-06-04].
- C4ADS (2019): ABOVE US ONLY STARS – Exposing GPS Spoofing in Russia and Syria. – Online in Internet: <https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf> [Stand: 2025-06-10].
- CAMERON, ALAN (2019): AFRL tests Chimera to battle spoofers and hackers. – Online in Internet: <https://www.gpsworld.com/afrl-tests-chimera-to-battle-spoofers-and-hackers/> [Stand: 2025-06-25].
- CARSTENSEN, JÖRG (2024): Kommt die Ukraine über einen Ringtausch an Marschflugkörper? – Online in Internet: <https://www.stern.de/politik/deutschland/taurus--kommt-die-ukraine-ueber-einen-ringtausch-an-marschflugkoerper--34397706.html> [Stand: 2025-06-05].

- CISA (Hrsg.): GLOBAL POSITIONING SYSTEM (GPS) INTERFERENCE. – Online in Internet: https://www.cisa.gov/sites/default/files/publications/CISA-Insights_GPS-Interference_508.pdf [Stand: 2025-06-22].
- CLEMENTS, ZACHARY & TODD E: HUMPHREYS (2023): Dual-Satellite Geolocation of Terrestrial GNSS-Jammers from Low Earth Orbi. – Online in Internet: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10140058> [Stand: 2025-06-22].
- DEPARTMENT OF DEFENCE (Hrsg.) (2021): DOD Dictionary of Military and Associated Terms. – Online in Internet: <https://irp.fas.org/doddir/dod/dictionary.pdf> [Stand: 2025-05-23].
- EISENHUT, CHRISTIAN (2025): Aufbau und Funktion eines Kompasses. – Online in Internet: <https://www.lernort-mint.de/physik/magnetismus/aufbau-und-funktion-eines-kompasses/> [Stand: 2025-06-28].
- EUROCONTROL (Hrsg.) (2022): TACAN network in Europe. – Online in Internet: <https://www.eurocontrol.int/sites/default/files/2022-09/erurocontrol-tacan-brochure-2022.pdf> [Stand: 2025-06-24].
- EUSPA (Hrsg.) (2021): BANSHEE - Hybridization of E-GNSS and WiFi ranging for LBS and automotive Accurate Navigation in Smart city. – Online in Internet: <https://www.euspa.europa.eu/opportunities/fundamental-elements/project-portfolio/banshee-hybridization-e-gnss-and-wifi-ranging> [Stand: 2025-06-26].
- FERRARA, DARLA (2025): The Definition of J/S Jamming in GPS. – Online in Internet: <https://itstillworks.com/definition-j-s-jamming-gps-12212859.html> [Stand: 2025-06-02].
- FINK, WILLI (2013): Satellitennavigation – Wunderwerk der Technik oder Waffe zur elektronischen Kriegsführung? – In: Wehrtechnik: WT, Ausgabe 45, Heft 2, 39-41.
- FREIMANN, GUSTAV (2024): Erfahrungen aus der Ukraine. Schutz gegen Drohnenbedrohung. – NAGY; KRISTOF & MARKUS REISNER (Hrsg.): Drohnenabwehr – Selbstschutz gegen Gefahren am Himmel Kampf mit Spähern und Angreifern, Wien, 73-97.
- FUTUREZONE (Hrsg.) (2025): Extrem genaue GPS-Alternative entwickelt. – Online in Internet: <https://futurezone.at/science/extrem-genaue-gps-alternative-entwickelt-quantennavigation-q-ctrl-traegheitsnavigation/403033455> [Stand: 2025-06-28].
- GELSEMA, SJOERD & RENE THAENS (2012): The Navigation Warfare Test Bed. – Online in Internet: <https://www.sto.nato.int/publications/pages/results.aspx?k=navigation%20warfare&s=Search%20All%20STO%20Reports> [Stand: 2025-05-23].
- GEWIES, STEFAN & RALF ZIEBOLD (2024): KI basierte Jamming Detektion mit verfügbaren GNSS Empfängern und R-Mode – Ein terrestrisches Backup-Positionierungssystem für die

- Schifffahrt. – Online in Internet: https://www.maritimes-cluster.de/fileadmin/user_upload/6_-_DLR_Gewies.pdf [Stand: 2025-06-27].
- GOTTIFREDI, FRANCO; CAPPELLA, MARCO; MARCINEK, KRZYSZTOF; ANTON, ALINA & BARBARA AMERIO (2022): ARGOS: a solution to increase security and safety of ships. – Online in Internet: https://indico.atenanazionale.org/event/5/papers/280/files/600-NAV2022_-_ARGOS_Solution_Paper_FINAL.pdf [Stand: 2025-06-25].
- GOWARD, DANA (2023): DHS Report on Denver Jamming – More questions than answers. – Online in Internet: <https://www.gpsworld.com/dhs-report-on-denver-jamming-more-questions-than-answers/> [Stand: 2025-06-21].
- GUSENBURGER, ERIC (2022): Drohnenabwehr aller Truppen? – Online in Internet: <https://soldat-und-technik.de/2022/03/bewaffnung/29577/drohnenabwehr-aller-truppen/> [Stand: 2025-06-05].
- HEIL, JULIA (2024): Nicht stören! – In: Jamming und Spoofing – wenn Stör- und Tauchsignale die Navigation beeinträchtigen, DLRmagazin 176. – Und Online in Internet: <https://www.dlr.de/de/medien/publikationen/magazine/alle-magazine-webversion/dlrmagazin-176/nicht-stoeren> [Stand: 2025-06-21].
- HOFFMANN, FELIX (o.J.): Was ist Avionik? – Online in Internet: <https://ninovalib.com/de/was-ist-avionik/> [Stand: 2025-06-21].
- HOPPE, MICHAEL (2017): GNSS-Anwendungen in der Schifffahrt. – In: GNSS 2017 – Kompetenz für die Zukunft, Beiträge zum 157. DVW-Seminar am 21. und 22. Februar 2017 in Potsdam, Band 87.
- HUMPHREY, TODD (2017). Part C GNSS Receivers and Antennas: 16. Interference. – In MONTENBRUCK, OLIVER & PETER J. G. TEUNISSEN (Hrsg.): Springer Handbook of Global Navigation Satellite Systems, 1. Auflage, 469–503.
- ILK, KARL HEINZ (2021): Satellitengeodäsie. – Grundlagen der Physikalischen und Mathematischen Geodäsie, Band 6, Bonn.
- ISLAM, SAIFUL; BHUIYAN, MOHAMMAD Z. H.; LIAQUAT, MUWAHIDA; PÄÄKKÖNEN, INTO & SANNA KAASALAINEN (2024): An open GNSS spoofing data repository: characterization and impact analysis with FGI-GSRx open-source software-defined receiver. – In: GPS-Solutions – The Journal of Global Navigation Satellite Systems, Ausgabe 28, Artikel 176. – Und Online in Internet: <https://link.springer.com/article/10.1007/s10291-024-01719-2> [Stand: 2025-06-10].

- JEKELI, CHRISTOPHER & OLIVER MONTENBRUCK (2017). Part A Principles of GNSS: 2. Time and Reference Systems. – In MONTENBRUCK, OLIVER & PETER J. G. TEUNISSEN (Hrsg.): Springer Handbook of Global Navigation Satellite Systems, 1. Auflage, 25–58.
- JONES, MICHAEL (2017): Anti-jam technology: Demystifying the CRPA. – Online in Internet: <https://www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/> [Stand: 2025-06-25].
- KASPER, WEST (2004): GPS vulnerability testing: Jamming and interference. – In: GPS world: news and applications of the global positioning system, Ausgabe 15, Heft 5, 20-27.
- KATHER, TIMO & OLE HENCKEL (2025): Faktencheck “Kamikazedrohne” _ Bundeswehr beschafft Loitering Munition. – Online in Internet: <https://www.bundeswehr.de/de/meldungen/bundeswehr-beschafft-loitering-munition> [Stand: 2025-06-21].
- KATO, TERUYUKI; TERADA, YUKIHIRO; NISHIMURA, HITOYOSHI; NAGAI, TOSHIHIKO & KOSHIMURA SHUN'ICHI (2011): Tsunami records due to the 2010 Chile Earthquake observed by GPS buoys established along the Pacific coast of Japan. – In: Earth, Planets and Space, Ausgabe 63, 5–8 und Online in Internet: <https://earth-planet-space.springeropen.com/articles/10.5047/eps.2011.05.001> [Stand: 2025-05-30].
- KERN, ESTER (2024): IT-Sicherheit von Weltraumsystemen. – In: NÖTZOLD, ANTJE; FELS, ENRICO, ROTTER, ANDREA & MORITZ BRAKE (HRSG.): Strategischer Wettbewerb im Weltraum – Politik, Recht, Sicherheit und Wirtschaft im All, Wiesbaden.
- KIESEWETTER, KLAUS D. (2024): Umfassende Analyse: GPS-Störungen im Ostseeraum und die Schatten des “Baltic Jammers”. – Online in Internet: <https://dasweltbild.de/europa/umfassende-analyse-gps-stoerungen-im-ostseeraum-und-die-schatten-des-baltic-jammers/> [Stand: 2025-06-12].
- KLEIN, THOMAS (2022): Mode-Navigation – The Future of Aeronautical Navigation. – Online in Internet: <https://www.mode-n.de/> [Stand: 2025-06-27].
- KPLER (2025): MarineTraffic Website. – Online in Internet: <https://www.marinetraffic.com/en/ais/home/centerx:-12.0/centery:25.0/zoom:4> [Stand: 2025-06-15].
- KO, KWANG-SOON (2010): A Basic Study on the Jamming Mechanisms and Characteristics against GPS/GNSS Based on Navigation Warfare. – In: Journal of Navigation and Port Research International Edition, Ausgabe 34, Heft 2, 97-103. – Und Online in Internet: <https://koreascience.kr/article/JAKO201023557658133.pdf> [Stand: 2025-06-03].
- KOELEMEIJ, JEROEN C.J.; DUN, HAN; DIOUF, CHERIF E.V.; DIERIKX, ERIK F.; JANSSEN, GERALD J.M. & Christian C. J. M. TIBERIUS (2022): A hybrid optical–wireless network for

- decimetre-level terrestrial positioning. – In: Nature, Ausgabe 611, S. 473-478. – Und Online in Internet: <https://doi.org/10.1038/s41586-022-05315-7> [Stand: 2025-05-27].
- KONOVALTSEV, ANDRIY; CUNTZ, MANUEL & ACHIM HORNBOSTEL (2017): Bedrohung von GNSS durch Jamming und Spoofing. – In: GNSS 2017 – Kompetenz für die Zukunft, Beiträge zum 157. DVW-Seminar am 21. und 22. Februar 2017 in Potsdam, Band 87. – Und Online in Internet: https://geodaesie.info/images/schriftenreihe/downloads/DVW_87_2017_GNSS_2017_FINAL_170206.pdf [Stand: 2025-05-13].
- KULPA, MIRKO (2004): Leistungsangaben bei WLAN-Komponenten. – Online in Internet: <https://www.nwlab.net/tutorials/db/eirp-umrechnung-dbm-mw.html> [Stand: 2025-06-03].
- KUNZI, FLORIAN (2023): LEO PNT als zukünftige Alternative in der globalen Satellitennavigation. – In: GNSS 2023 – Zeit für ein Update?! – Beiträge zum 219. Seminar der INTERGEO akademie am 4. und 5. September 2023 in Bochum. – Und Online in Internet: https://geodaesie.info/images/schriftenreihe/downloads/DVW_106_2023_GNSS_2023_FINAL_230816.pdf [Stand: 2025-06-04].
- KUUSNIEMI, HEIDI (2022): Robust GNSS+: PNT Innovation for Autonomous Vehicles. – Online in Internet: https://navisp.esa.int/uploads/files/documents/Keyspeaker_Robust%20GNSS+,%20PNT%20Innovation%20for%20Autonomous%20Vehicles.pdf?v=250998 [Stand: 2025-06-19].
- LANGLEY, RICHARD B.; WEAVER, BRADON; ZAMPIERI, GIANLUCA & OKUARY OSECHAS (2021): Innovation: Mode N provides alternative PNT for aviation. – Online in Internet: <https://www.gpsworld.com/innovation-mode-n-provides-alternative-pnt-for-aviation/> [Stand: 2025-06-28].
- LICKTEIG, JANA (2023): Orientierung im Gelände: Karte, Höhenmesser & Kompass richtig lesen. – Online in Internet: <https://www.bergzeit.de/magazin/orientierung-mit-karte-und-kompass-anleitung/?msockid=15c8d1a2a8e26a3f32abc393a9256b26> [Stand: 2025-06-28].
- LUBER, STEFAN (2025): Was ist ein Global Navigation Satellite System (GNSS)? – Online in Internet: <https://www.ip-insider.de/was-ist-ein-global-navigation-satellite-system-gnss-a-58b68ef95a2f0e31d0eaab8fea60fdeb/> [Stand: 2025-05-13].
- LUCCIO, MATTEO (2022): The transition to M-code begins. – Online in Internet: <https://www.gpsworld.com/the-transition-to-m-code-begins/> [Stand: 2025-05-14].
- LOCKHEED, MARTIN (2019): GPS III: The Next Big Step in GPS Modernization. – Online in Internet: <https://insidegnss.com/gps-iii-the-next-big-step-in-gps-modernization/> [Stand: 2025-05-29].

- LUFTFAHRTMAGAZIN (Hrsg.) (2025): R-Mode: Satellitenunabhängige Navigation auf der Ostsee. – Online in Internet: <https://www.luftfahrtmagazin.de/raumfahrt-technik/satelliten/r-mode-satellitenunabhaengige-navigation-auf-der-ostsee-259839.html> [Stand: 2025-06-27].
- MAJOHR, JÜRGEN & MARTIN KUROWSKI (2021): Maritime Regelungs- und Sensorsysteme – Automatisierte Schiffsführung – mit MATLAB und Simulink. – Rostock.
- MANSFELD, WERNER (2010): Satellitenortung und Navigation – Grundlagen, Wirkungsweise und Anwendung globaler Satellitennavigationssysteme. – 3. Auflage, Wiesbaden.
- MEURER, MICHAEL (2024): CCG-Seminar SE 3.25 – Robustheit und Störbarkeit von Satellitennavigation, unveröffentlicht.
- MITCH, RYAN H.; DOUGHERTY, RYAN C.; PSIAKI, MARK L.; POWELL, STEVEN P. & BRADY W. O'HANLON (2011): Signal Characteristics of Civil GPS Jammers. – Online in Internet: <https://repositories.lib.utexas.edu/items/293e1da1-b2fc-4184-ae12-6e81452bca05> [Stand: 2025-06-04].
- MÜLLER, ACHIM (2008): Satellitengestützte Positionierung und Navigation in der Bundeswehr. – In: Europäische Sicherheit: Politik, Streitkräfte, Wirtschaft, Technik, Band 57, Heft 1, 68-72.
- NAGY, KRISTOF (2024): Im Kampf gegen Kleindrohnen. – NAGY; KRISTOF & MARKUS REISNER (Hrsg.): Drohnenabwehr – Selbstschutz gegen Gefahren am Himmel Kampf mit Spähern und Angreifern, Wien, 37-72.
- NATO (2008): STANAG-4621 – NAVIGATION WARFARE DEFINITION. – Online in Internet: <https://publishers.standardstech.com/content/military-dod-stanag-4621> [Stand: 2025-05-23].
- NÖTZBOLD, ANTJE (2024): Die sicherheitspolitische Bedeutung von Weltraum und NewSpace im Ukraine-Krieg – politische Implikationen für die militärische und kommerzielle Raumfahrtnutzung. – In: SIRIUS – Zeitschrift für Strategische Analysen, Band 8, Heft 2, 202-221 – Und Online in Internet: <https://www.degruyterbrill.com/document/doi/10.1515/sirius-2024-2004/html> [Stand: 2025-05-13].
- OERTEL, ROBERT; NIPPOLD, ROLAND; RÜGAMER, ALEXANDER; SCHMIDT, WILLI; SCHUSTER, JÜRGEN & JAN WENDEL (2022): HALI-Berlin: Emergency vehicle preemption with Galileo PRS. – Online in Internet: <https://elib.dlr.de/186924/1/ITS%20Toulouse%202022%20HALI%20Berlin%20elib.pdf> [Stand: 2025-06-25].
- PELTORA, PEKKA & TERRY MORE (2017): Towards Seamless Navigation. – In: NURMI, JARI; LOHAN, ELENA-SIMONA; WYMEERSCH, HENK; SECO-GRANADOS, GONZALO & OSS

- NYKÄNEN (Hrsg.): Multi-Technology Positioning, S. 125-147. – Und Online in Internet: https://doi.org/10.1007/978-3-319-50427-8_7 [Stand: 2025-06-26].
- POHL, LINA (2024): Die Auswirkungen des Krieges in der Ukraine auf den Raumfahrtsektor und Implikationen für Europa. – NÖTZOLD, ANTJE; FELS, ENRICO, ROTTER, ANDREA & MORITZ BRAKE (HRSG.): Strategischer Wettbewerb im Weltraum – Politik, Recht, Sicherheit und Wirtschaft im All, Wiesbaden.
- OFFSHORE ENGINEERING (Hrsg.) (2021): DP – Dynamic Positioning. – Online in Internet: <https://www.offshoreengineering.com/dp-dynamic-positioning/what-is-dynamic-positioning/> [Stand: 2025-06-26].
- RAWNSELEY, ADAM (2011): Iran's Alleged Drone Hack: Tough, but Possible. – Online in Internet: <https://www.globalsecurity.org/org/news/2011/111216-iran-drone-2.htm> [Stand: 2025-07-11].
- REISNER; MARKUS (2024): Die Kalaschnikows der Lüfte. – NAGY; KRISTOF & MARKUS REISNER (Hrsg.): Drohnenabwehr – Selbstschutz gegen Gefahren am Himmel Kampf mit Spähern und Angreifern, Wien, 73-97.
- RETERSKI, MILOSZ (2015): Jamming session: hackers target global geonavigation networks. – In: Jane's Intelligence review, Ausgabe 27, Heft 3, 32-36.
- ROBOT MAKERS (Hrsg.) (2021): Was ist Odometrie? – Online in Internet: <https://robotmakers.de/glossar/odometrie/> [Stand: 2025-07-14].
- ROHDE&SCHWARZ (Hrsg.) (2023): RESILIENT POSITIONING NAVIGATION AND TIMING BASED ON 5G BROADCAST. – Online in Internet: https://navisp.esa.int/uploads/files/project_documents/NAVISP2-EL2-112_Final_Presentation_v2.pdf?v=497380 [Stand: 2025-06-27].
- RÖNNBERG, NILS (2020): Sextant: Funktion einfach erklärt. – Online in Internet: https://praxistipps.chip.de/sextant-funktion-einfach-erklaert_117331 [Stand 2025-06-28].
- ROPER, TONY (2019): Jamming arrays. – In: Jane's intelligence review, Ausgabe 31, Heft 8, 26-31.
- SAALBACH, KLAUS (2025): Kriegsführung mit GPS (Navigation Warfare). – Online in Internet: https://osnadocs.ub.uni-osnabrueck.de/bitstream/ds-2025012612091/1/GPS_Navigation_Warfare_2025_Saalbach.pdf [Stand: 2025-05-27].
- SAAPWOOD, OLIVIA (2024): Intelligence officers burned the Russian R-330Zh Zhitel EW system. – Online in Internet: <https://militaryni.com/en/news/intelligence-officers-burned-the-russian-r-330zh-zhitel-ew-system/> [Stand: 2025-06-10].

- SCHLIPPERT, DENNIS (2019): Quantum Inertial Navigation Systems – The "direction signs" of the future. – Online in Internet: <https://www.iqo.uni-hannover.de/de/arbeitsgruppen/guidedmatterwaveinterferometry/quantum-inertial-navigation-systems> [Stand: 2025-06-28].
- SCHMIDT, GEORGE T. (2013): Navigation Sensors and Systems in GNSS Degraded and Denied Environments. – Online in Internet: <https://www.sto.nato.int/publications/STO%20Educational%20Notes/Forms/Educational%20Notes%20Document%20Set/docsethomepage.aspx?ID=3132&FolderCTID=0x0120D5200078F9E87043356C409A0D30823AFA16F60300099FA443AE6E08499A57A0FBE0134F20&List=44a8f49d-e481-458a-91b4-212a9605bd9e&RootFolder=https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-SET-197> [Stand: 2025-06-03].
- SCHÜTTLER, TOBIAS (2022): Satellitennavigation – Wie sie funktioniert und wie sie unseren Alltag beeinflusst. – Technik im Fokus, 2., aktualisierte und erweiterte Auflage, Habach.
- SCHUH, H.; WICKERT, J.; DICK G.; GE, M.; RAMATSCHI, M.; LI, X.; DENG, Z.; ALSHAWAF, F.; ARRAS, C. & B. MÄNNEL (2017): Der Beitrag von GNSS zum Monitoring des Systems Erde. – In: GNSS 2017 – Kompetenz für die Zukunft, Beiträge zum 157. DVW-Seminar am 21. Und 22. Februar 2017 in Potsdam, Band 87. – Und Online in Internet: https://geodaesie.info/images/schriftenreihe/downloads/DVW_87_2017_GNSS_2017_FINAL_170206.pdf [Stand: 2025-05-13].
- SCHWEBER, BILL (2020): Magnetic-Field Navigation as an "Alternative" GPS? – Online in Internet: <https://www.electronicdesign.com/markets/automation/article/21145842/electronic-design-magnetic-field-navigation-as-an-alternative-gps> [Stand: 2025-06-27].
- SKAI DATA SERVICES (Hrsg.) (2025a): The World's First Live GPS Spoofing & Jamming Tracker. – Online in Internet: <https://gpswise.aero/> [Stand: 2025-06-24].
- SKAI DATA SERVICES (Hrsg.) (2025b): GPSwise: Mitigating GPS Spoofing & Jamming Risks in Aviation – White Paper. – Online in Internet: <https://gpswise.aero/spoofing-ui/white-paper> [Stand: 2025-06-25].
- SPEKTRUM (Hrsg.) (2000): astronomische Ortsbestimmung. – Online in Internet: <https://www.spektrum.de/lexikon/geowissenschaften/astronomische-ortsbestimmung/1023> [Stand: 2025-06-28].
- SOKOLOV, DANIEL AJ (2020): GPS – Der "magische Kompass" mit gewollter Ungenauigkeit. – Online in Internet: <https://www.heise.de/hintergrund/GPS-Der-magische-Kompass-mit-eingebauer-Ungenauigkeit-4713291.html> [Stand: 2025-06-02].

- STANSIAK, MIRKO; VON HÜNERBEIN, KAREN; BESTMANN, ULF & WERNER LANGE (2016): Measured GNSS Jamming Events at German Motorways. – Online in Internet: https://www.researchgate.net/publication/304462554_Measured_GNSS_Jamming_Events_at_German_Motorways [Stand: 2025-06-21].
- SÜß, JULIANA (2024): Weltraumkapazitäten im Ukraine Krieg. – In: SIRIUS – Zeitschrift für Strategische Analysen, Band 8, Heft 1. – Und Online in Internet: <https://www.degruyterbrill.com/document/doi/10.1515/sirius-2024-1006/html> [Stand: 2025-06-06].
- TASDEMIR, EMRAH; KURZ, LOTHAR & TOBIAS G. NOLL: Combined spatial-temporal filtering for interference mitigation in GNSS receivers. – In: European journal of navigation: the leading journal for systems, services and applications, Ausgabe 12, Heft 2, S. 4-9.
- THEDARTHDESIGNER (2019): BEST Anti Ballistic Missile / Anti Satellite Weapon Systems in the World | ABM Top 10. – Online in Internet: <https://www.youtube.com/watch?v=hz8TuE9n2sk> [Stand: 2025-05-29].
- TRIEBERT, CHRISTIAAN; MIGLIOZZI, BLACKI; CARDIA, ALEXANDER; XIAO, MUYI & DAVID BOTTI (2023): Fake Signals and American Insurance: How a Dark Fleet Moves Russian Oil. – Online in Internet: <https://www.nytimes.com/interactive/2023/05/30/world/asia/russia-oil-ships-sanctions.html> [Stand: 2025-05-13].
- UNMANNED NETWORK (2023): UVision Air launches revolutionary Hero-90: a portable tactical loitering munition system with anti-strike capabilities, for dismounted soldiers. – Online in Internet: <https://unmanned-network.com/uvision-air-launches-revolutionary-hero-90-a-portable-tactical-loitering-munition-system-with-anti-strike-capabilities-for-dismounted-soldiers/> [Stand: 2025-06-21].
- VAL, LAURA (2022): BANSHEE - Hybridization of E-GNSS and Wi Fi ranging for LBS and automotive Accurate Navigation in Smart city. – Online in Internet: <https://www.euspa.europa.eu/sites/default/files/banshee.pdf> [Stand: 2025-06-27].
- WAGNER, ROLAND (2023): Vorlesung vom 10.10.2023 im Rahmen des Moduls Geoinformatik an der Berliner Hochschule für Technik. – Online in Internet: <https://drive.google.com/file/d/1DFnPpzfF3HC5PQQMpg3VR8LBGUoRgtEG/view?usp=sharing> [Stand: 2025-06-24].
- WESTBROOK, TEGG (2019): The Global Positioning System and Military Jamming: The geographies of electronic warfare. – In: Journal of Strategic Security, Ausgabe 12, Heft 2, Artikel 1. – Und Online in Internet: <https://www.jstor.org/stable/26696257?seq=11> [Stand: 2025-06-04].
- WISEMANN, JOHN (2022): GPSJAM. – Online in Internet: <https://gpsjam.org/> [Stand: 2025-06-12].

ZHANG, ZHENG; GONG, XIAOPENG; GU; SHENGFENG, ZHENG, FU & YIDONG LOU
(2025): Analysis of GPS satellite flex power in 2023 and its effects on differential code bias variations. – In: GPS Solutions – The Journal of Global Navigation Satellite Systems, Ausgabe 29, Artikel 91. – Und Online in Internet: <https://doi.org/10.1007/s10291-025-01849-1> [Stand: 2025-06-02].

Die Abbildungen, welche geändert oder erstellt wurden, wurden mit www.canva.com erstellt.